Corr. US 2002/0042884 A1

P 56

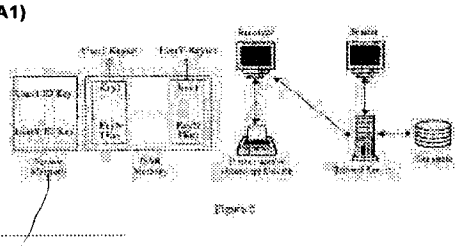
Secreting and/or discriminating documents remote-controlling printing

Publication number: CN1348130 (A)
Publication date: 2002-05-08
Inventor(s): JIANKANG WU [SG]; BAOSHI ZHU [SG]; QUNYING ZHU [SG] +
Applicant(s): ZHUOXIN SCIENCE & TECHNOLOGY C [SG] +
Classification:
- international: ***B41J29/00; B41J29/38; B41J5/30; G06F1/00; G06F12/14; G06F21/00; G06F21/20; G06F21/24; G06F3/12; G09C1/00; H04L29/06; H04N1/44;*** **B41J29/00; B41J29/38; B41J5/30; G06F1/00; G06F12/14; G06F21/00; G06F21/20; G06F3/12; G09C1/00; H04L29/06; H04N1/44;** (IPC1-7): G06F12/16; G06F3/12; H04L9/00
- European: G06F21/00N9C2; H04L29/06C8; H04L29/06S12A; H04L29/06S6B; H04L29/06S8C
Application number: CN20011025933 20010716
Priority number(s): SG20000005827 20001011

Also published as:
CN1252581 (C)
EP1197828 (A1)
US2002042884 (A1)
WO0232047 (A1)
JP2002169681 (A)
more >>

Abstract not available for CN 1348130 (A)
Abstract of corresponding document: **EP 1197828 (A1)**

A method for the remote printing of a document by use of a network, the method including receiving at a server the document as sent from a sender; the server forwarding the document to a recipient; the document being authenticated prior to being forwarded to the recipient; and the server receiving instructions from the sender regards printing controls and the server implementing those controls on the recipient. A hardware device to support the printing controls is also disclosed.



[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
G06F 3/12
H04L 9/00 G06F 12/16

[12]发明专利申请公开说明书

[21]申请号 01125933.7

[43]公开日 2002年5月8日

[11]公开号 CN 1348130A

[22]申请日 2001.7.16 [21]申请号 01125933.7
[30]优先权
[32]2000.10.11 [33]SG [31]200005827-1
[71]申请人 卓信科技有限公司
地址 新加坡恒穆肯巷21号
[72]发明人 吴健康 朱保实 朱群英 黄 晟

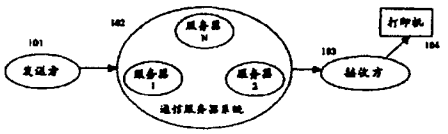
[74]专利代理机构 北京市柳沈律师事务所
代理人 马 莹

权利要求书7页 说明书35页 附图页数12页

[54]发明名称 保密和/或鉴别文件的远控打印

[57]摘要

一种借助网络远控打印文件的方法，其包括以下步骤：(a)在服务器上接收从发送方处发送来的文件；(b)服务器将文件转送给接收方；(c)在转送给接收方之前鉴别该文件；(d)服务器从发送方处接收有关打印控制的指令，服务器还实现接对收者 处的控制。同时也公开了一种支持打印控制的硬件设备。



ISSN1008-4274

权　利　要　求　书

1.一种借助网络远控打印文件的方法，其包括以下步骤:

(a)在服务器上接收从发送方处发送来的文件;

(b)服务器将文件转送给接收方;

(c)在转送给接收方之前鉴别该文件;

(d)服务器从发送方处接收有关打印控制的指令，服务器还实现对接收方的控制。

2.一种借助网络远控打印文件的方法，其包括以下步骤:

(d)发送方将文件发送到服务器，使服务器能将文件转送给接收方;

(e)在将文件发送到服务器之前，由发送方鉴别文件;

(f)将用于控制文件打印的指令发送给服务器，使服务器能实现对接收方的控制。

3.一种打印鉴别文件的方法，该文件是借助网络从远端接收到的，该方法包括如下步骤:

(c) 服务器从发送方处已接收鉴别的文件后，接收方从服务器接收鉴别的文件;

(d) 服务器从发送方接收到打印控制，服务器实现对接收方的打印控制。

4.根据权利要求1-3中任一项所述的方法，其中，打印控制包括保证使该文件打印出来的内容与发送方发送的文件内容严格一样。

5.根据权利要求1-4中任一项所述的方法，其中，打印控制包括防伪造控制。

6.根据权利要求1-5中任一项所述的方法，其中，打印控制包括防复制控制。

7.根据权利要求1-6中任一项所述的方法，其中，打印控制包括控制需打印文件的份数

8.根据权利要求1-7中任一项所述的方法，其中，接收方包括一个打印机，服务器向用于打印文件的打印机提供打印控制。

9.根据权利要求1-8中任一项所述的方法，其中，服务器使文件能保密地从发送方通过服务器发送给接收方。

10.根据权利要求1-9中任一项所述的方法，其中，服务器在打印控制中是发送方的可信代理。

11.根据权利要求1-10中任一项所述的方法，其中，服务器是在验证文件服务中的可信的第三方。

12.根据权利要求11所述的方法，其中，服务器可储存文件的散列信息和文件的至少一个内容特征，并用它们来验证文件。

13.根据权利要求11或12所述的方法，其中，保密文件的发送和打印控制基于可信文件结构的基础上，该可信文件包括以下组合中的一个或多个的部分：

a)文件自身；

b)手写签名；

c)数字标记；

d)光学水印；

e)文件的内容特征；

f)使用控制和核查跟踪；

g)发送方的封印；

h)终止日期。

14.根据权利要求11-13中任一项所述的方法，其中，发送方核准文件。

15.根据权利要求1-14中任一项所述的方法，其中，该方法可使用公用密钥结构来保证在文件传送过程中的认可、保密和安全性。

16.根据权利要求13或14所述的方法，其中，文件上可使用数字标记，该数字标记是从发送方、服务器和接收方组成的组合中选择的一个或多个的数字标记。

17.根据权利要求1-16中任一项所述的方法，其中，发送方可在发送文件之前利用服务器注册。

18.根据权利要求1-17中任一项所述的方法，其中，在接收方可接收文件之前利用服务器注册。

19.根据权利要求14-18中任一项所述的方法，其中，用于确认的文件散列信息和内容特征可与文件一起发送，散列信息和文件的内容特征保持在服务器中，以便于以后验证。

20.根据权利要求1-13中任一项所述的方法，其中，该方法可使用由保密接口层协议所提供的保密文件发送信道；通过利用用户身份和至少一个口令鉴别发送方和接收方。

21.根据权利要求1-13中任一项所述的方法，其中，该方法也可使用用于保密文件传送的加密技术。

22.根据权利要求21所述的方法，其中，给文件解密的密钥通过一个运载装置直接送到接收方，该运载装置是从下列组合中选出的：电子邮件、电话、邮件、快递和专有传送装置。

23.根据权利要求1-22中任一项所述的方法，其中，打印文件通过使用鉴别装置可得以保护，而防止未授权的复制和伪造，所述鉴别装置是从下列组合中选出的：光学水印、特殊墨水、特殊纸张和特殊打印材料。

24.根据权利要求23所述的方法，其中，光学水印可具有一个防假冒层。

25.根据权利要求24所述的方法，其中，检验打印机以实现防假冒层的高级性能。

26.根据权利要求25所述的方法，其中，可使用打印语言来执行检验，不需要手写干预。

27.根据权利要求8-26中任一项所述的方法，其中，打印机在打印控制过程中可以是保密的。

28.根据权利要求27所述的方法，其中，打印机可包括一个保密存储器、保密中央处理单元和保密时钟。保密存储器可用来储存专有密钥；保密中央处理单元可用来防止运行中攻击，保密时钟可用来计时。

29.根据权利要求27所述的方法，其中，打印机和服务器系统使用公用密钥对或打印机的对称密钥构成的组合中选择的一个或多个，来执行保密信号交换，以鉴别彼此身份。

30.根据权利要求27所述的方法，其中，服务器可发送一个加密文件散列信息、光学水印和打印指令给打印机。

31.根据权利要求30所述的方法，其中，打印机可通过客户软件接收文件，给文件解密，在打印之前利用散列信息和时间标志核对文件，并在打印期间增加光学水印。

32.根据权利要求28-31中任一项所述的方法，其中，在打印之后，立即从保密存储器上将该文件删除。

33.根据权利要求8-32中任一项所述的方法，其中，还包含的步骤有在服务器中生成核查跟踪记录。

34.根据权利要求1-26中任一项所述的方法，其中，还包括客户软件，为了打印文件，被下载到接收方的机器上。

35.根据权利要求34所述的方法，其中，在打印控制过程中接收方是可信的，以减少对客户软件攻击。

36.根据权利要求35所述的方法，其中，服务器通过客户软件与打印机通信，来验证打印机系列号和内部协议地址，核对打印机状态，锁定打印机的控制板，设置所有必要的打印机参数，将要打印的文件和用来打印文件的指令发送给打印机，在完成打印后重设打印机参数，并在服务器中生成核查跟踪记录。

37.根据权利要求13所述的方法，其中，封印包括从由手写签名和封印构成的组合中选择的一个或多个；该封印包括对所有打印文本来讲都是共用的共用封印，以及对每个打印副本来讲是唯一的独特封印。

38.根据权利要求34-36中任一项所述的方法，其中，客户软件有一个基本部分和高度机密部分，当接收方利用服务器注册时，高度机密部分比基本部分更容易受到攻击，该基本部分被传送到接收方，高度机密部分下载到接收方机器上，用于打印文件，并在打印完后，从接收方机器上删除，以便于防止高度机密部分受到攻击。

39.根据权利要求38所述的方法，其中，当接收方利用服务器注册时，将高度机密部分的加密形式发送给接收方，该服务器管理解密密钥；需要时，将高度机密部分解密。

40.根据权利要求38或39所述的方法，其中，基本部分的散列信息结果可在与基本部分被发送给接收方的同时或之前取得，该散列信息结果储存在服务器中；当接收方需要打印文件时，取得基本部分的第二散列信息结果，并在由服务器授权打印之前与散列信息结果比较。

41.根据权利要求38-40中任一项所述的方法，其中，用于执行高度机密部分中的一些部分的执行时间记录在服务器里，并与打印文件时的执行该部分的时间相比较；如果花费的时间显然比执行时间长，则中止打印。

42.根据权利要求1-41中任一项所述的方法，其中，响应于接收方打印文件的请求，执行打印控制。

43.根据权利要求1-26中任一项所述的方法，其中，打印控制可脱机进行，服务器不参与打印过程。

44.根据权利要求43所述的方法，其中，在接收方提供了硬件设备，来代表服务器起作用。

45.根据权利要求44所述的方法，其中，硬件设备控制文件打印，该硬件设备包括保密存储器、读后删除存储器、具有单片程序的中央处理单元以及端口；硬件设备利用服务器注册。

46.根据权利要求43或44所述的方法，其中，该机器可包括打印机、与打印机是一个整体的硬件设备；该打印机利用服务器注册。

47.根据权利要求45所述的方法，其中，保密存储器含有一个可访问存储器，只有当输入并核对用户口令时才可访问该存储器，而且只能访问与用户相关的可访问存储器的一个块；还含有用于内部使用的可控存储器，该可控存储器被分成许多块，对每个用户有一可控存储器块。

48.根据权利要求47所述的方法，其中，可控存储器用于保存保密密钥、系列号、用户专有密钥和接收方ID密钥。

49.根据权利要求13-48中任一项所述的方法，其中，控制包括发放打印文件的许可证给接收方，该许可证包括授权打印文件的副本份数。

50.根据权利要求49所述的方法，其中，每个许可证有一个许可证密钥，该许可证密钥用于给独特封印加密；所述许可证密钥以加密形式由服务器发送给接收方并被安装在硬件设备中。

51.根据权利要求50所述的方法，其中，服务器可增加许可证密钥的数量，服务器产生新许可证密钥集和新添加密钥，在将通过服务器发送到接收方并安装在硬件设备里之前，该新许可证密钥集和新添加密钥用先前的添加密钥加密。

52.根据权利要求49-51中任一项所述的方法，其中，每个许可证密钥可包括一个终止日期，在该日期后，就不可以再使用许可证打印文件。

53.根据权利要求51所述的方法，其中，新许可证密钥集与文件分开发送。

54.根据权利要求51所述的方法，其中，新许可证密钥集与文件一起发送。

55.根据权利要求49-52中任一项所述的方法，其中，在发送方发送文件之前，可用第一会话密钥对发送方的共用封印、用于发送的时间标志和终止日期进行加密，以给出一个加密结果。

56.根据权利要求55所述的方法，其中，加密结果和文件可利用第二会话密钥加密，以给出第二加密结果。

57.根据权利要求56所述的方法，其中，在第二加密结果中，包括有一个散列信息结果，以提供一种用于核对数据完整性的方式。

58.根据权利要求49-57中任一项所述的方法，其中，打印控制可访问文件，但不打印文件，还可访问许可证，访问许可证时不用要求。

59.根据权利要求13-58中任一项所述的方法，其中，在授权打印文件之前，核对终止日期，如果终止日期已过，则不再允许打印。

60.根据权利要求1-59中任一项所述的方法，其中，发送方和服务器是一样的，发送方的所有功能都由服务器执行。

61.根据权利要求60所述的方法，其中，发送方有权发放保密硬件设备给每个接收方，通过网络将文件和许可证密钥发送到每个接收方，每个接收方使用保密硬件设备打印文件，该文件作为打印或电子文件，由接收方发送给接收方的消费者，保密硬件设备控制电子文件的发送，保密硬件设备进行核查跟踪，并且当添加新许可证密钥时将它发送到管理机构。

62.根据权利要求61所述的方法，其中，文件由邮票、税务发票、税务收据构成的组合中选择。

63.根据权利要求62所述的方法，其中，邮票、税务发票、税务收据每个的数值被包括在核查跟踪中。

64.根据权利要求63所述的方法，其中，根据被包括于核查跟踪中的数值，管理机构可以决定应当支付的税款。

65.根据权利要求43-64中任一项所述的方法，其中，还提供了一种保密软件程序，用来执行接收方的打印控制。

66.根据权利要求65所述的方法，其中，该软件程序以一个分散的形式执行，以有助于防止软件攻击。

67.根据权利要求66所述的方法，其中，用于许可证密钥和核查跟踪的保密存储器以一个分散的形式来实现。

68.一种与用户机一起使用的硬件设备，其可控制至少一个由该用户机执行的文件打印，该硬件设备包括一个保密存储器、读后删除存储器、具有单片程序的中央处理单元，和一个接口。

69.根据权利要求68所述的硬件设备，其中，保密存储器含有一个可访问存储器，只有当输入并核对用户口令时才可访问该存储器，而且只能访问与用户相关的可访问存储器中的一个块；还含有分成许多块的可控存储器，每个用户具有一可控存储器。

70.根据权利要求69所述的硬件设备，其中，可控存储器用于存储保密密钥、系列号、用户专有密钥和接收方ID密钥。

71.根据权利要求68-70中任一项所述的硬件设备，其中，硬件设备可借助保密软件程序实现。

72.根据权利要求71所述的硬件设备，其中，该保密软件程序可以分散的形式执行，以有助于防止软件攻击。

说　明　书

保密和/或鉴别文件的远控打印

技术领域

本发明涉及一种用于控制保密和/或经鉴别(authenticaed)的文件的打印的方法和设备，尤其涉及，但不仅限于，这样一种包括能控制打印过程的方法和设备。

定义

在该说明书中，文件是指包括电子或打印形式的文件。

在该说明书中，鉴别(authencation)包括保密，反之亦然。

在该说明书中，机器包括桌上型计算机、膝上型计算机、笔记本计算机或其它合适形式的计算机。

在该说明书中，“打印”包括对文件各种形式的处理，包括：打印、查看、收听、保存、电子形式的发送、转送和类似功能。

背景技术

在经营商业和管理行业通常要使用纸件文件。虽然不断预计要无纸化办公，但是在数字时代依然可见办公用纸增加。主要原因在于这样更可靠。当文件由管理人员正确签署时，他们的签名就具有认证性。无论签名出现在何时何地，有人都能在一定程度上确定文件的真实性。众所周知，正因为严格控制原始文件的数量，才实现了保密。

美国专利US6,091,507涉及一种在网络上打印文件的方法和设备。其利用网络协议、传输格式、硬件接口，便于从具有光栅图象处理器的主机将光栅数据高速地传送到打印机。显然，它不能访问与文件相关的许多重要课目，该文件是保密的，并可信(trusted)或经鉴别(authenticated)的。

美国专利US5,983,065涉及一种打印保密文件的方法。其使用一种可控访问电子打印机来打印原始文件。由此形成的打印图象在可见光中可以识别出，并由标记材料（液体油墨和/或干色粉）所生成，该材料至少包含光活性

（courmarin）化合物。被打印的原始文件图象不能在通常复印机上复制或扫描仪上扫描。其使用特殊打印材料。

美国专利US5,917,996公开了一种使用防篡改技术、结合电子形式特征打印防篡改文件的方法，其披露了保密的背景技术。

美国专利US6,085,181公开了一种邮资计量系统，作为仪表服务器用于在网络上进行可独立应用的仪表工作。打印机组件在网络上作为客户打印机模式操作，该网络连接到邮政保密设备（PSD）。该PSD包括独特的标识符、邮资值储存器和数字标记发生器。客户打印机通过当地客户打印机组件，请求从PSD获得邮资支付的证据，用于结束邮资计量办理。邮资支付的证据包括与每个请求邮资支付的证据相关的数字标记。该专利提供了对邮资的使用控制方式。

在现有技术中，没有公开两个重要问题：文件复制份数控制，文件的鉴别控制。

本发明的主要目的是提供一种用于远控打印鉴别文件的方法和设备，所述打印能够加以控制。

发明内容

基于上述目的和别的目的，本发明提供了一种借助网络来远控打印文件的方法，该方法包括以下步骤：

(a)在服务器上接收从发送方(sender)处发送来的文件；

(b)服务器将文件转送给接收方(recipient)；

(c)文件在转送给接收方之前进行鉴别；

(d)服务器从发送方接收有关打印控制的指令，服务器还在接收方执行那些控制。

本发明还提供一种用于借助网络远程打印文件的方法，该方法的步骤包括：

(a)发送方将文件发送到服务器，使服务器能将文件转送给接收方；

(b)在将文件发送到服务器之前，由发送方鉴别文件；

(c)将用于控制文件打印的指令发送给服务器，以便使服务器能实现对接收方的控制。

本发明还以另一种形式提供了一种打印鉴别文件的方法，该文件是借助网络远程接收到的，该方法的步骤如下：

(a) 服务器从发送方接收到经鉴别的文件后，接收方从服务器接收经鉴别的文件；

(b)服务器从发送方接收到打印控制后，服务器实现对接收方的打印控制。

打印控制最好包含保证能使打印出来的内容与发送方发送的文件内容一样，和/或防伪造控制和/或防复制控制和/或能控制被打印文件的副本份数。

接收方可包括一个打印机，为了打印文件，发送方向打印机提供打印控制。服务器最好使文件能保密地从发送方通过服务器发送到接收方，并在打印控制中是发送方的可信代理。服务器也可以是验证文件的可信第三方。为了做到这些，服务器可使用储存在服务器里的散列信息(hash)和文件的内容特征。可基于可信文件结构发送保密文件和打印控制，该结构包括一个或多个的：

a)文件自身；

b)手写签名；

c)数字标记；

d)光学水印；

e)文件的内容特征；

f)使用控制和核查跟踪(audit trail)；

g)发送方的封印(seal)；

h)终止日期。

发送方可能是有权处理文件的人。该方法可使用公用密钥结构来保证在文件传送过程中的认可(non-repudiation)、保密和安全性。

数字标记可用到文件上，数字标记是发送方、服务器和接收方的数字标记。发送方和接收方最好在发送和接收之前分别利用服务器注册。文件散列信息和内容特征可与用于确定的文件一起发送，散列信息和文件的内容特征保持在服务器中，以便于以后验证。

该方法可使用保密接口层协议(Secure Socket Layer protocol)所提供的保密文件转送通道；通过使用用户身份和至少一个口令鉴别发送方和接收方。

该方法也可使用用于保密文件传送的加密技术。因此，给文件解密的密钥通过一个运载装置被直接送到接收方，该运载装置是从下列构成的组合中选出的：电子邮件、电话、邮件、快递和专有传送装置。

打印文件通过使用鉴别装置可得以保护，而防止未授权的复制和伪造，该装置是从下列构成的组合中选出的：光学水印、特殊墨水、特殊纸张和特殊打印材料。

光学水印可具有一个防假冒层。打印机可被检验来实现防假冒层的高级性能。可使用打印语言来执行检验，不需要人为干预。此外，打印机在打印控制过程中可以是保密的；可包括一个保密(secure)存储器、保密中心处理单元、和保密(secure)时钟。保密存储器可用来储存专有密钥；保密中心处理单元可用来防止运行中受攻击(attack)，保密时钟可用来计时。最好，打印机和服务器使用公用密钥对或打印机的对称密钥，来执行保密信号交换，以鉴别彼此身份。

服务器可发送一个加密文件散列信息、光学水印和打印指令给打印机。

打印机可接收来自客户软件的文件，给文件解密，在打印之前利用散列信息和时间标志核对文件，并在打印期间增加光学水印。

最好，打印机在打印之后，就将文件立即删除；并在服务器中进行核查跟踪记录。

接收方在打印控制过程中或许是可信的，在这种情况下，服务器可通过客户软件与打印机通信，来验证打印机系列号和互联网协议地址，核对打印机状态，锁定打印机的控制板，设置所有必要的打印机参数，将要打印的文件发送给打印机，在完成打印后重设打印机参数，并在服务器中进行核查跟踪记录。

封印(seal)可包括由以下构成的组合中选择出的一个或多个：手写签名和封印；封印包括对所有打印副本来讲都是公用的共用封印，以及对每个打印副本来讲是唯一的独特封印。

客户软件有一个基本部分和高度机密部分，当接收方利用服务器注册时，该基本部分被传送到接收方，高度机密部分比基本部分更容易受到攻击。高度机密部分下载到接收方机器上，以便于打印文件，并在打印完后，从接收方机器上删除，以便于防止高度机密部分受到攻击。当接收方利用服务器注

册时，最好能将高度机密部分的加密形式发送给接收方，该服务器管理解密密钥；需要时，将高度机密部分解密。

基本部分的散列信息结果可在与基本部分发送给接收方的同时或之前取得，该散列信息结果储存在服务器中；当接收方需要打印文件时，取得基本部分的第二散列信息结果，并在服务器授权打印之前与散列信息结果比较。

客户软件可储存在接收方的硬件设备中。

作为一种选择方式或附加方式，用于高度机密部分元件执行的执行时间可记录在服务器里，并与打印文件时的元件执行时间相比较；如果花费的时间显然比执行时间长，则中止打印。

最好，响应于接收方打印文件的请求执行打印控制。打印控制可脱机(off-line)进行，服务器不参与打印过程。在那种情况下，在接收方提供了硬件设备，起服务器和/或保密软件程序的作用，执行对接收方的打印控制。最好，软件程序以一个分散的形式来执行，以便于防止软件受到攻击。

发送方和服务器可以是一样的，此时，服务器执行所有发送方的功能。

硬件设备可控制文件打印，该硬件设备包括保密存储器、读后删除存储器、具有单片程序的中央处理单元以及接口；硬件设备要利用服务器注册。机器可包括打印机、与打印机是一个整体的硬件设备；该打印机要利用服务器注册。

保密存储器可含有一个可访问存储器，只有当输入并核对用户口令时才可访问该存储器，而且只能访问与用户相关的可访问存储器的那一块(block)；还含有用于内部使用的可控存储器，该可控存储器被分成多个块，每个用户一个可控制存储器块；可控存储器用于存储保密密钥、系列号、用户专有密钥和接收方ID密钥。

控制可包括发放打印文件的许可证给接收方，许可证包括授权打印文件的副本份数。每个许可证最好有一个许可证密钥，该许可证密钥用于将独特封印加密；所述许可证密钥以加密形式由服务器发送给接收方并被安装在硬件设备中。服务器可添加许可证密钥，服务器产生了新许可证密钥集和新添加(top up)密钥，在通过服务器被发送到接收方并被安装在硬件设备里之前，用先前的添加密钥对所述新许可证密钥集和新添加密钥加密。

每个许可证可包括一个终止日期，在该日期后，就不可以再使用许可证打印文件。新许可证密钥集可与文件分开或一起发送。

在发送方发送文件之前，发送方的共用封印、用于发送的时间标志和终止日期，可用第一会话密钥加密，以给出一个加密结果。然后该加密结果和文件可利用第二会话密钥加密，以给出第二加密结果；在第二加密结果中，包括有一个散列信息结果，以提供一种用于核对数据完整性的措施。

打印控制可查看文件，但不打印文件，查看不要求许可证。终止日期最好在授权打印文件之前核对，如果终止日期已过，则不再允许打印。

发送方有权发放保密硬件设备给每个接收方，通过网络将文件和许可证密钥发送到每个接收方，每个接收方使用保密硬件设备打印文件，该文件作为打印或电子文件，由接收方发送给接收方的消费者，保密硬件设备控制电子文件的发送，保密硬件设备进行核查跟踪信息，并且当添加新许可证密钥时将它发送给管理机构。

文件可以是邮票、税务发票和/或税务收据，在核查跟踪中包括其数值。管理机构可基于包括核查跟踪中的数值决定其应当支付的税款。

按另一种形式，本发明还提供了一种硬件设备，与用户机器一起使用，使其至少可控制利用该机器的一个文件的打印，该硬件设备包括一个保密存储器、读后删除存储器、具有单片程序的中央处理单元和一个接口。

该保密存储器可含有一个可访问存储器，只有当输入并核对用户口令时才可访问该存储器，而且只能访问与用户相关的可访问存储器的那一块；还含有可控存储器，被分成许多块，每个每个用户有一个存储器块。可控存储器可用于存储保密密钥、系列号、用户专有密钥和接收方ID密钥。硬件设备可借助保密软件程序实现，该保密软件程序可以分开的形式执行，有助于防止软件攻击。

附图说明

为了可以更好地理解本发明，以及容易地实现本发明，在此，将参考以下附图，并借助非限制性的本发明最佳实施方式进行说明：

附图1是一个文件发送和打印系统的方块图。

附图2描述了一个可信(trusted)文件的结构。

附图3是控制打印机的流程图，该打印机使用PJL语言。

附图4是用于脱机打印的硬件设备的方块图。

附图5是第一脱机打印方案的方块图。

附图6是用于图5所示方案的文件数据格式。

附图7表示了添加(top up)密钥集的生成。

附图8是图7所示添加过程的流程图。

附图9是第二脱机打印方案的流程图。

附图10是用于图9所示方案的文件数据格式。

附图11是用于图9和图10所示方案的许可证和许可证安装数据格式。

附图12是用于脱机打印的第二硬件设备的方块图。

附图13是第三脱机打印方案的图表。

附图14是用于图13所示方案的文件数据格式。

附图15表示了添加密钥集的生成。

附图16是图15所示的添加过程的流程图。

附图17是第四脱机打印方案的方块图。

附图18是用于图17所示方案的文件数据格式。

附图19是用于图17和图18所示方案的许可证和许可证安装数据格式。

附图20是用于基于软件脱机打印的密钥数据库。

附图21是用于基于软件脱机打印的密钥挽救文件。

附图22是基于软件脱机打印方案的方块图。

附图23是用于基于软件脱机打印的许可证和许可证安装数据格式。

附图24是用于基于软件脱机打印方案的文件数据格式。

具体实施方式

本发明有三个主要部分：所有文件的转送和打印过程，其中，服务器系统起可信第三方的作用；鉴别打印文件的装置；以及其自身的打印控制。

所有文件的转送和打印过程

参考附图1，保密远控文件打印系统有四个主要部分。文件发送方应该是有权利启用文件的人。通信服务器系统至少包括一个服务器，该服务器为保密可靠的文件发送提供必要设备。在鉴别发送方时其起可信第三方和接收方的作用，这个办理是基于内部公用密钥基础结构（PKI）协议的基础上的。并且还起代表发送方的可信媒介的作用，以便执行发送方的打印请求，并控制打印过程。打印过程通过接收方网点常驻的软件，由通信服务器系统控制。至于使用加密技术的保密文件发送，请参考ISO/CCITT X400，至于PGP，例

如参见1995年由C.Kaufman,R.Perlman和M.Speciner,PTR Prentice Hall写的网络安全-在公共世界中的专有通信。

在文件转送中，文件将具有如图2所示的结构，该结构使其成为一个可信文件。加上文件本身，还包括五个其它的部分：

● 手写签名和/或发放管理机构的封印(seal)，立即给人一种值得信任的感觉。只有管理机构鉴别成功时将手写签名和封印加到文件上。用这种方式，手写签名才有意义。

● 文件的数字标记，该数字标记是为了认可(no repudiation)和内容完整性的目的由发送方、接收方和服务器系统建立的。数字标记是利用专有密钥的文件散列信息的加密。由所有三方的数字标记将保证起源、接收和发送的认可性。

● 在文件上的光学水印保证对文件的鉴别，保护文件不被复制和伪造。

● 文件的内容特征是由整个文件整个文件中提取出的，用来验证文件的内容，并查找可能变化的位置，为了将来对文件进行验证，被存储在服务器系统中。

● 使用控制和核查跟踪记录维持管理机构的使用说明，也决定拷贝控制的执行状态，并由服务器系统管理。

有三种操作程序选择，每一个都有不同等级的保密性：

a)基于PKI的高保密性操作程序，它为用户鉴别和认可提供了一种措施；

b)保密发送，使用的是保密接口层(Secure Socket Layer)（SSL）协议；

c) 使用对称加密的保密发送。

基于PKI的高保密性操作程序

注册

所有用户（发送方和接收方）都利用服务中心注册，该中心管理通信服务器系统。注册操作程序包括，但不仅限于：

● 用户要求注册，并提供他们的证明，用户身份（“ID”），要求的服务类型，以及从公共证明管理机构（如果可能的话）获得的数字证明；

● 然后服务中心验证用户证据，产生一个用户简档(profile)，并将该简档储存在其注册数据库中。然后服务中心产生一个注册身份，并将信息和可信客户软件转送给用户。如果用户没有数字证明，内部证明管理机构将通过以下步骤发送一个数字证明给用户：

-内部证明管理机构产生一个消息鉴别代码（“MAC”）密钥，并将它与客户软件和注册身份一起发送给用户；

-用户使用客户软件产生一个密钥对，以产生一个关于证明的请求，并用MAC密钥给它加密，送到服务中心。专有密钥可能被储存于用户机器中的硬盘、软盘、只读光盘、智能卡或任何其它合适的装置上；

-然后服务中心验证请求、传输信号，并将用户证明返回。同时，服务中心将用户证明的副本存放在证明数据库中；

-服务中心在硬拷贝上打印用户证明的手印，并且，服务中心和注册用户都在硬拷贝上签名。

发送文件

为了使发送方将文件发送到接收方，可采取以下步骤：

●发送方通过提供它们的注册ID、权标（即便要）和口令，注册进入服务器系统；

●服务器系统验证发送方的身份，如果验证成功，则提示接收方姓名、地址、待发送的文件以及允许由接收方打印的副本复制份数。如果具有所要求的ID的接收方存在于服务中心的数据库中，服务器系统就从证明数据库中提取公用密钥证明，产生一个唯一系列号，并记录下办理时间。整个办理过程所花的时间可被忽略。如果接收方没有利用服务中心注册，客户软件就产生一个会话密钥，用会话密钥给数据加密，用口令给会话密钥加密，并通过单独的电子邮件、电话或其它形式发送口令。

●发送方验证接收方的证明、ID和办理时间。然后，发送方的客户软件计算要发送文件的散列信息、附加系列号、时间、发送方ID和接收方ID，使用发送方专有密钥签名，并将其发送到服务中心；

●服务器系统核对签名的真实性，并产生它自己的签名；

●发送方验证服务器系统的签名，并将它合并在文件中；

●用户的客户软件将发送方的手写签名、发送方公司的封印和文件的内容特征加到文件中；使用服务器系统的证明给内容特征和散列信息加密，使用接收方的证明给其余信息和散列信息加密，并将它下载到服务器系统；

●接收到加密文件时，服务器系统就将它存储在证据数据库中，并发一个通知给接收方。在一预定时期内为了鉴别文件，将散列信息和内容特征储存在服务器中。

接收文件

步骤如下：

●服务器系统将可得到的文件通知接收方，还传送文件ID和文件系列号；

●接收方用接收方ID、权标（即便要）和口令在服务器系统上注册；

●服务器系统核对有效性，产生系列号、时间、发送方ID和接收方ID的散列信息。对这些签名并将签名和散列信息发送给接收方。发送方的证明、加密文件和发送方的签名也和这些信息一起发送；

●然后接收方验证发送方的公用密钥证明，给文件解密，产生散列信息，并反复查对由服务器系统发送来的生成散列信息。如果它们匹配，验证成功。验证还包括服务器系统的发送时间；

●接收方的客户软件产生文件散列信息、系列号、接收方ID、发送方ID和时间的混杂信号的签名，并送到服务器系统。这将使服务中心能完全相信文件已经被成功解密；

●然后服务器系统验证该信息，并将有关信息储存在证据数据库中；

●当接收方提出打印请求时，服务器系统就通过客户软件，与在接收方网址的打印机通信，并核对其状态。如果打印机准备好了，服务器系统就将文件和用于打印的光学水印发出去。如果没有错误消息，打印就会成功。服务器系统引起核查跟踪去记录整个过程；

●服务器系统将确认信息发送给接收方，通知发送方。

使用SSL保密传送

SSL（保密接口层）协议，正如1999年RFC2246第1版“传送层保密”，在两方之间提供了一个保密信道。所有通过SSL信道的数据转送都将使用会话密钥加密，会话密钥是为每一个联系随机地产生。发送步骤是：

●发送方和服务器系统建立联系，保密地交流SSL会话密钥，以下所有的办理都是经过加密信道的；

●发送方用它们的注册ID和口令在系统上注册；

●服务器通过它们的注册ID和口令验证发送方身份；

●然后发送方提出请求发送数据（可能是文件）给接收方；

●服务器确认请求，并准备接收数据；

●发送方将数据与散列信息和内容特征一起发送；

● 一接收到数据，服务器系统就将它储存在证据数据库中，并给接收方发通知。在一预定时期内，散列信息和内容特征将被储存在服务器中，用来为以后的鉴别服务；

● 当接收方接收到通知时，就利用客户软件，与服务器建立联系，并交流SSL会话密钥。所有以下处理都经过加密信道；

● 然后接收方在系统上用他们的注册ID和口令注册；

● 服务器验证接收方的注册ID和口令，如果核实，则服务器将把数据传送给接收方；

● 接收方接收数据，并向服务器发送确认信息；

● 如果接收方提出发送打印经鉴别副本的请求，则服务器将用散列信息和内容特征验证文件，并与打印机通信，而且发送文件和用于打印的光学水印，还引起核查跟踪来记录整个过程的状态。

用加密技术保密传送

● 发送方用它们的注册ID和口令在服务器上注册；

● 服务器验证发送方的注册ID和口令；

● 发送方提出发送数据（又可能是文件）的请求；

● 服务器确认请求，并准备从发送方接收数据；

● 发送方从数据中产生一个散列信息和内容特征，并产生一个随机会话密钥来给数据加密。密钥和散列信息用口令加密，散列信息和内容特征用服务器系统的公用密钥加密，然后，下载到服务器系统；

● 服务器系统接收被加密的数据、密钥、散列信息和内容特征，并将它们存在数据库中；

● 然后发送方通过电话、电子邮件、邮件、个人递送或其它方式将口令通知接收方；

● 当接收方接收到来自发送方的口令时，接收方利用注册ID和口令注册进入服务器；

● 服务器验证注册ID和口令，如果核实，则将加密数据、密钥和散列信息发送给接收方；

● 接收方接收加密数据、密钥和散列信息，并给服务器发送接收确认；

● 接收方使用单独获得的口令给密钥和散列信息解密，并用密钥给数据解密；

● 接收方计算被解密数据的散列信息，并将它与接收到的散列信息比较。如果它们一样，则又将确认发送给服务器；

● 如果接收方向管理机构提出打印经鉴别文件的请求，则服务器系统核对发送方定义的数据库记录，以了解它们是否被允许打印文件，以及他们被允许打印多少副本。如果符合，服务器系统就利用散列信息验证文件，与打印机通信，并发送用于打印的文件和光学水印。还引起核查跟踪来记录打印状态。

文件鉴别的措施

任何合适的装置都能用来鉴别文件，例如，特殊墨水和特殊纸张都以控制方式使用。另一个例子是使用具有多层嵌入实物图象的光学水印。光学水印图象被存储在服务器系统中，并转送到打印机，以便于以一种由服务器系统以控制方式来打印文件。在文件上的光学水印在某种意义上来说提供了一种可靠性，如果没有得到服务器系统的允许就打印文件的话，文件上是没有光学水印的，因此，文件是无效的。光学水印在我们的共同申请PCT/SG00/00147中已经公开，申请的标题为“光学水印”，是2000年9月15日在新加坡申请的，因此在此将其内容作为参考。

光学水印可保护文件不被假冒和伪造，它将多个实物潜像嵌入多层重复结构中，产生一个水印。然后水印被合并到文件中，例如，作为一个封印，标识图或背景。这会被称作一个光学水印。

在光学水印中的防假冒层对打印机的属性很高度机密。具体说，它取决于可由影印机探测的像点大小。为了保证光学水印的打印效果，有必要有个校准过程，来决定最小可见像点的大小和其最佳嵌入的空间频率。这个过程可能包括：

● 产生一排具有不同像点大小的测试图案的阵列；

● 用户从打印测试页中，确定第一可见测试图案数量，以便于找到打印机能打印的最小可见像点；

● 基于这个数量，系统产生并打印具有不同频率的测试图案的阵列；

● 用户从这个打印页中，确定第一可见测试图案数量，以便于找到能够最好隐藏信息的频率；

● 利用这两个数量，打印确认页；

● 用户影印确认页。如果可以看见防复制特征了，就完成检验。否则再次执行检验，直到获得成功的结果。

打印控制

打印控制提供了一个控制过程，以确保文件严格按照管理机构/发送方的指令打印。就是说，当管理机构/发送方发送文件时，也输入了他们的打印指令。然后该指令由服务器系统实施，作为一个可信媒介，服务器系统将指令作为文件转关历史的一部分储存到数据库中。该服务器系统将根据发送方提供的指令控制打印过程。服务器系统控制打印过程的方式有很多种。

已存在的打印过程不具有任何控制。当客户从服务器接收到文件时，文件由一个卷筒系统送到网络打印机。一旦打印请求纳入在卷筒行列中，打印请求和客户/服务器之间的链路投入使用。唯一的消息就是打印请求是否成功。人们可容易地获得数据，并请求打印机打印多份副本。

由于服务器系统可信和保密，服务器系统通过客户软件和打印机通信。为了确保控制打印过程，可用到很多方法，包括接收方。所使用的方法将是不同的，并对于不保密打印机和/或非保密接收方来讲又是不同的。

保密打印机的打印控制

保密打印机将具有一个硬件单元，该硬件单元包括一个时钟；一个用来储存加密密钥和储存用来为数据加密和解密的程序的保密存储器；一个执行程序、与客户和服务器通信并控制打印机的CPU。该硬件单元在这种意义上是保密的，即可以防止外部对时钟、密钥、程序和运行程序的攻击。当用户请求管理机构打印鉴别文本时，服务器系统与打印机通信，完成与客户的信号交换过程。打印机和服务器系统根据公用密钥对鉴别成功后，服务器系统就将加密后的散列信息和光学水印与时间标志、打印指令一起发送给打印机。关于保密信号交换协议和加密数据发送的细节，参考由C.Kaufman , R.Perman , 和M . Speciner , PTR Prentice Hall在1995年所著的“网络安全-在公共世界中的专用通信”第223页第9章“安全信号交换缺陷”。

打印机将其专有密钥保存在保密储存器中。当接收方利用服务中心注册时，服务器系统就知道了其数字证明。在成功地完成保密信号交换过程后，服务器系统将加密指令、文件散列信息和光学水印一起发送给打印机。所有数据都用时间标志和数字标记加密。打印机接收到来自客户软件的文件，为数据解密，验证来自服务器的数字标记和时间标志，如果验证成功就打印。

打印完后，数据立即被删除。打印机产生打印数据的散列信息，并将散列信息和时间标志签名，并将它发送给服务器，保存在核查跟踪记录中。

由于加密技术和PKI，在服务器和打印机之间的通信就很安全。保密打印机由可信厂商生产和检查，以确保储存在保密存储器中的程序不会被篡改，并防止对打印机CPU中运行的程序运行进行攻击。

可信客户的打印控制

当客户是可信分的时候，应该不会对客户软件引起攻击，也不会对客户软件程序产生运行中攻击。通过客户软件，服务器系统与打印机通信，核对其状态，发送打印指令和数据，监视整个过程，并最后进行核查跟踪记录。与打印机的对话使用可获得的打印任务语言，例如，由Hewlett Packard写的PJL和PML。图3是使用PJL的打印控制流程图。在打印控制过程中的主要步骤是:

- 核对并记录打印机的IP地址、系列号;
- 读出打印机的状态，包括对所有打印任务都是共同的打印机设置，也包括只对特定打印任务才有效的打印机设置，以及以固定间隔如每15秒的打印机状态;
- 设置对于所有当前打印任务需要的必要设置的数值;
- 锁定控制板，防止当打印任务发送到打印机时，另一个用户利用该设置篡改。如果控制板不能被锁定，打印任务就被异常终止;
- 利用附录(PS) 、打印控制语言（PCL）或爱普生标准打印机代码（ESC/P）发送打印任务。

控制程序将首先获得所有关于打印机设置的必要信息。有了这个信息，将非所需的结构或设置改成所需的设置。然后打印机以预定的间隔如每15秒向回报告设备和页数的细节。接下来，将打印任务发送给打印机。利用经常的状态报告，打印过程得以严密监视。如果打印纸发生堵塞，就汇报出错误，再打印一次。打印完成后，打印机设置改回到原始设置。获取所有的状态报告供核查跟踪。

检验过程不必人工干预。就是说，在工厂里就执行了检验过程，比较可见像点大小、色粉等级和其它打印机参数。利用这些数据，在核对打印机状态后，就决定并设置了合适的打印机参数，以便于将最好性能的光学水印打印在文件上。

有非保密打印机的非保密客户的打印控制

非保密客户和非可信客户可能意味着可能会对客户软件和硬件和打印机产生攻击。这些包括对软件的攻击，运行中攻击以获取数据，向服务器提供错误信息。有两个途径：一个是有尽可能防病毒的客户软件，另一个是设置另外硬件单元来保护客户软件。客户软件当分发时被划分成两部分，基本部分和高度机密部分。高度机密部分包含高度机密的代码和数据，如产生功能和访问控制的水印。当用户注册时，分发并安装基本部分。

保护客户软件的方法包括：

● 为每个打印验证基本客户软件。

任何对客户软件的修正都可能会引起客户软件发生故障。这样的修正可由网络错误、用户硬盘错误、或对软件的攻击引起。为了防止这一点，在发送软件之前计算基本客户软件的散列信息结果并储存在服务器中。当用户请求打印时，计算相同的散列信息功能，将结果发送到服务器中用于验证。只有当散列信息结果与以前储存的结果相同时，该服务器才将打印数据发送给客户。否则，不允许打印，促使用户采取进一步行动。

● 根据请求下载高度机密代码，或还运行中将高度机密代码解密。

高度机密部分保存在可信服务器中，或以加密格式发送给客户。当被保存在可信服务器中时，需要时便利用基本部分通过保密连接（例如SSL）下载到客户PC，并在使用后立即被删除。高度机密部分很小，或被压缩，以便于减少下载时间。高度机密部分也可与客户软件基本部分一起安装在客户机器中，只不过是以加密形式。需要时，高度机密部分载于存储器中，解密并被执行。服务器管理解密密钥。通过这种办法，如分解代码的静态攻击就不可能的了。

● 从硬件中获得高度机密部分。

攻击者实际上会不定时地攻击客户软件，但攻击硬件困难得多。因此，可能在打印过程中由硬件获得高度机密部分,并且打印过程一结束，就从存储器中抹去。一个熟练的攻击者可成功地攻击客户软件，并无约束地打印文件，但是由于没有鉴别光学水印，所以这些副本都明显无效。

● 探测运行中攻击

一个运行中攻击方法是用调试程序调试该程序。由于一些先进的调试程序能够避免探测，所以在运行系统时搜索调试程序是不合适的。探测运行中攻击的一个有效方法是计算高度机密功能的执行时间。如果程序被调试的话，

该执行时间会显著低于正常值。产生一个单独的线索来监视那些高度机密功能的执行时间。如果时间明显长于应有时间，则中断主要过程。

另一个运行中攻击的方法是用挂机系统监视系统呼叫活动。当系统功能呼叫被挂机时，其所有输入和输出数据都被废弃，这些数据可能包括解密数据或机密信息。为了防止这种攻击，客户软件将列举出所有系统挂机，并将它们与内部黑名单相比较。如果发现列入黑名单的挂机，客户软件将中断运行。服务器会经常更新前述的黑名单，处理新出现的挂机申请。

脱机打印控制

当打印控制是脱机时，所有要求打印文件的信息在打印前被下载到客户机。其最好包括:

● 文件自身;

● 一个封印，包括一个手写签名和/或一个发送方的物理封印图象，以及一个光学水印。该封印进一步被分成两部分：一个是与所有文件打印副本共用的共用封印，；另一个是每一个文件打印副本特有的独特封印;

● 使用控制和核查跟踪。

该信息以一种特定加密文件包的形式发送，以确保其加密性。由于服务器不参与打印过程，所以保密硬件/软件被安装到代表服务器的客户系统中去起服务器的作用。因此，这样就提供了两种方案-硬件方案和软件方案。如前所述，它们可能独立运用，也可能结合使用。

硬件方案

参考图4，保密硬件设备被连接到客户系统，最好与打印机成一整体。该设备最好包括:

1.一个保密存储器（401），其用于储存重要信息。由CPU以及其单片程序（403）设置不同的访问权限。例如，有两种存储器:

a)当输入并验证了用户口令时，可访问的存储器;

b)严格控制内部使用的存储器。例如，保密密钥和/或系列号被储存在存储器中。系列号最好由硬件厂商保证是唯一的。

2.一个DAR（读后删除）存储器（402）。在该存储器上的数据在读后自动删除。其可通过单片程序或硬件达到。重要信息，例如打印许可证，被储存在该区域;

3.具有单片程序（403）的CPU，其可能访问保密存储器401和DAR存储器402，鉴别用户请求，加密，解密，并产生数字标记。单片程序也包括一个密钥管理系统，最好是一个文件系统。当打印任务下达时，任务识别号就发送到硬件设备，在那儿密钥管理系统从保密存储器401或DAR存储器检索相应密钥。该CPU也可包括一个保密实时时钟，来防止时间方面攻击；

4.接口（404）。它负责在硬件设备和主机之间建立通信，也为数据流加密，以防止分接攻击。

在硬件设备中的存储器空间，保密存储器和DAR存储器两个都被分成几块(block)。一个合格的用户只能通过正确的口令访问属于他们的块。设计该设备包括一定数量的块，该块具有用来访问这些块的最初口令，这些块在存储器芯片生产时就分配好了。一个独特的用户ID密钥存储在用于每一个接收方的保密存储器块中，并被记录在服务器的数据库中。当使用数字证明时，用户专有密钥能够被储存在硬件设备400的保密存储器块中。

无论使用其CPU还是用打印机的CPU（如果可以获得的话），硬件设备400都应该能执行加密/解密操作。

该服务器是可信的，负责让用户可利用硬件，并管理密钥和硬件设备的其它方面。

硬件设备通过许多方案中的一种方案来控制打印，现在举两个例子来说明：

方案1:

该方案使用了对称加密技术，例如，3DES，AES，Blowrish等等。它包括发送方(sender)、接收方(receiver)、打印设备和可信服务器，如图5所示。接收方的硬件设备具有许多组随机密钥（密钥1，...密钥N，T密钥），被写在它们的块DAR存储器中。T密钥代表一个添加密钥，这些密钥是许可证密钥，并被用于给独特的封印加密。这些添加密钥（T密钥）被用在添加过程中。该组独特的用户ID密钥和与每一个密钥对应的初始口令保存在硬件设备的保密存储器中。这些密钥的副本也保存在可信服务器中。发送方和接收方，还有它们的硬件设备也必须在使用保密打印过程之前利用可信服务器注册。

接收方的注册过程

接收方应该在接收文件之前利用可信服务器注册。注册过程可包括：

1.接收方通过提供他们的信息，如用户名、电子邮件、和他们硬件设备的ID等，请求在服务器注册；

2.服务器处理接收方的请求。如果批准，服务器就在其数据库中搜寻未使用的硬件设备的用户ID。如果所有用户ID都被使用了，则安装一个新的硬件设备；

3.服务器记录用户信息，并发送初始口令和用户ID索引给接收方；

4.如果没安装客户软件的话，将客户软件安装到接收方的机器上；

5.接收方通过输入他们的用户名、初始口令和用户ID索引注册到客户软件；

6.将用户ID索引和初始口令发送到硬件设备，以便于为用户启动其相应的块；

7.提示接收方立即改变他们的口令，用新口令取代原始口令；

8.客户软件为用户准备一个专有目录，并将该目录的密钥（称做目录密钥）存储到硬件设备中的用户的存储块里。

许可证密钥添加过程

正如图6-8所示，当用户已使用储存在设备中的许可证密钥，或当对于新请求的许可证不足时，用户将有必要添加他们的许可证密钥，步骤如下：

1.当服务器接收到发送方的请求，将一个文件的M个许可证密钥发送给接收方，并且服务器发现用于接收方完成任务的许可证密钥不足时，服务器会启动添加过程；或者

2.接收方请求添加他们的许可证密钥，例如由于，如接收方不具有足够的密钥，所有的接收方密钥都用过了，或接收方想打印更多的副本；

3.然后，服务器处理该请求。如果批准的话，服务器就产生一组新的密钥密钥1'- 密钥X'，和一个新的添加密钥（T密钥'）；

4.该组新的密钥用接收方的T密钥加密；

5.为该组新的密钥计算散列信息，并利用接收方的ID密钥将其与新密钥集加密，以形成添加密钥集；

6.添加密钥集与文件包一起或单独地发送给接收方；

7.在接收方接收到该数据后，接收方将添加密钥集发送给硬件设备；

8.该设备用接收方的ID密钥给数据解密，并为核对完整性而计算数据的散列信息；

9.如果数据有错误，该设备则从DAR存储器读取T密钥'来给密钥集解密；

10.然后该设备更新DAR存储器中的密钥集。该新的密钥集将不改写未使用的密钥，由于它的索引号数从先前最后的密钥继续；

11.在DAR存储器中的先前的添加密钥（T密钥）由新添加密钥T密钥'来取代。

发送方将文件发送给接收方：

1.使用他们的用户ID和口令发送方通过保密联系链路（如SSL）连接到可信服务器；

2.鉴别成功后，发送方准备他们的文件：

a)使用会话密钥1给文件或它的散列信息结果、共用封印、用于发送的时间标志以及文件的终止日期加密；

b)为文件主体、终止日期和步骤a)的结果计算散列信息结果，然后这三部分用会话密钥2加密；

c)然后将步骤b)的结果、接收方的ID、会话密钥1、用做加密的会话密钥2、允许接收方打印文件的M份副本许可证数量（如M）以及M个独特封印发送给服务器。M可能是0，表示仅仅阅览；

3.服务器核对接收方信息，然后随机地或顺序地从接收方密钥集中选择M个许可证密钥（Key1-KeyM）；

4.M个独特封印和会话密钥1各用Key1-KeyM加密，形成M个许可证。计算整个许可证包的散列信息域以保证对许可证核对完整性；

5.然后服务器产生一个文件包（图6），该包包括发送方准备好的文件主体（上面步骤2中（b）的结果）、用接收方ID密钥加密的会话密钥2以及许可证。如果发送方不允许接收方打印文件，许可证领域将是空的。如果接收方的许可证密钥不够时，也预备好添加密钥集；

6.服务器发这通知给接收方，建议他们准备收集文件包。

接收方接收到上述（6）的通知之前或之后的任何时间，接收方都能连接到服务器。然后接收方能核对是不是有给他们的数据。

接收方查看并打印文件的操作程序如下：

1.接收方利用他们的用户名和口令，通过保密链路（如SSL）连接到可信服务器；

2.服务器通过发送询问响应系列验证用户：

a)服务器验证用户名，然后从数据库检索用户ID密钥；

b)服务器选择或产生随机号，利用用户ID密钥加密，并向回发送给接收方。

c) 将接收方的口令发送给硬件设备，以访问他们的ID密钥；

d)硬件设备使用ID密钥给已加密的随机号解密；

e)将随机号向回发送服务器；

f)服务器通过验证随机号来鉴别用户；

3.鉴别成功后，客户软件从服务器为接收方下载数据；

4.接收到数据后，接收方可断开服务器，或保持在线状态；

5.客户软件核对是否有添加密钥集。如果有，则为了添加许可证密钥，首先将添加密钥集发送到设备；

6.客户软件将加密会话密钥2发送到该设备用于解密。将会话密钥2解密，并返回客户软件，该客户软件给文件包解密，并核对文件包中的散列信息域。如果核对失败，接收方通知服务器这个决定，此时，加密文件或它的散列信息、共用封印、时间标志和终止日期都没有解密；

7.然后文件包重新加密并使用目录密钥将其储存在接收方的专有目录中。

当接收方想查看文件时，执行以下操作程序：

1.接收方使用他们的用户名和口令注册到客户软件，并由硬件设备鉴别；

2.鉴别成功后，客户软件读取接收方的目录密钥，并访问接收方的专有文件包的专有目录；

3.将终止日期与硬件设备的内部时钟比较，如果内部时钟显示出终止日期已过去，则文件已经期满，不再允许查看；

4.如果文件没有期满，则接收方能查看文件。

当接收方希望打印文件时，执行以下操作步骤：

1.接收方使用他们的用户名和口令注册到客户软件，并由硬件设备鉴别；

2. 鉴别成功后，客户软件从硬件设备中读取接收方的目录密钥，并访问接收方的专有文件包的专有目录；

3 客户软件将一个未使用过的许可证发送给硬件设备用于解密；

4 硬件设备根据索引从接收方的DAR存储器读取密钥，并给会话密钥1和独特封印解密；

5 文件或其散列信息、共用封印、时间标志、终止目期被发送给该设备用于解密。将终止目期与该设备中的时钟比较，如果内部时钟显示出终止目期已过，则文件已经逾期，不再允许打印；如果设备上的硬件有故障，用户应该通知硬件发放者来解决问题；

6 客户软件利用上述步骤（5）的解密文件散列信息验证文件的完整性，并将文件发送到打印机，或将解密文件发送到打印机；

7 客户软件与打印机通信，监视打印状态，将具有正确的封印的文件打印出来；

8 在每打印一份副本后，就进行核查跟踪信息，并由具有接收方ID密钥的硬件设备内的程序签名，保证认可每个打印副本；

9 将核查跟踪信息储存在硬件中，并定期装载到服务器。在预定时期内，服务器保持核查跟踪。在预定时期结束后，就从服务器删除。

方案2:

参考图9，当硬件设备中的DAR存储器制造出来时是空的（记为零）。所有必要密钥的副本也储存在可信服务器中。所有发送方和接收方以及他们的硬件设备，必须在它们能进行保密打印过程之前，利可信服务器用注册。

接收方的注册过程与方案1介绍的一样，包括:

1.发送方使用他们的用户ID和口令通过保密链路（如SSL）连接到可信服务器；

2.鉴别成功后，发送方准备他们的文件:

a)使用会话密钥1给文件或它的散列信息结果、共用封印、用于发送的时间标志以及文件的终止目期加密；

b)为文件主体、终止目期和步骤a)的结果计算散列信息结果，然后这三部分用会话密钥2加密；

c)然后将步骤b)的结果、接收方的ID、会话密钥1、用于加密的会话密钥2、关于接收方打印M份副本的许可证数量以及M个独特封印发送给服务器。M可能是0，表示只能查看；

3.服务器核对接收方信息，然后产生一个许可证和许可证安装程序，如图11所示；

4.许可证包含会话密钥1和M个独特封印，该M个独特封印用服务器随机地产生的M个许可证密钥密钥1-密钥M进行加密；

5.许可证安装程序包含一个用于文件的独特ID，也包含一个时间标志（此时，产生许可证安装程序）和终止日期，该许可证安装程序是由接收方ID密钥加密的；

6. 也计算许可证和许可证安装程序的散列信息，以核对其完整性；

7.然后服务器产生一个文件包，如图10所示，该包包括发送方准备好的文件包（上面步骤2中（b）的结果）、用接收方ID密钥加密的会话密钥2以及许可证、许可证安装程序。如果发送方不允许接收方打印文件，许可证和许可证安装程序的域(field)将是空的；

8.服务器通知接收方，告诉他们该文件可得到以便收集。

不管接收到还是没有接收到任何类似的通知，接收方都能连接到服务器，核对是不是有给他们的文件和/或数据。接收方查看并打印文件的操作程序如下：

1.接收方利用他们的用户名和口令，通过保密链路（如SSL）连接到可信服务器；

2.服务器通过发送询问响应系列验证用户：

a)服务器验证用户名，然后从数据库检索用户ID密钥；

b)服务器产生随机号，利用用户ID密钥对随机号加密，并发送给接收方。

c) 将接收方的口令发送给接收方的硬件设备，以访问他们的ID密钥；

d)接收方的硬件设备使用ID密钥将已加密的随机号解密；

e)将随机号向回发送服务器；

f)服务器通过验证随机号来鉴别用户；

3.鉴别成功后，客户软件接收方从服务器下载文件和/或数据；

4.接收到文件和/或数据后，接收方可断开服务器，或保持在线状态；

5.客户软件将许可证安装程序发送给接收方硬件设备，以实现安装；

6.硬件设备使用接收方ID密钥将许可证安装程序解密，并通过验证散列信息域而核对许可证安装程序的完整性。如果验证失败，则接收方通知服务器解决问题；

7.该设备利用保存的ID列表，核对文件ID；

8.如果没发现ID，就依靠设备中的时钟核对时间标志和终止日期；

9.如果所有核对操作程序完成得都很成功，则许可证密钥就被安装在接收方DIR存储器中，并且将ID储存在保密存储器的ID列表中；

10.客户软件将加密会话密钥2发送到该硬件设备用于解密。该硬件设备将会话密钥2解密，并将其返回客户软件，该客户软件给文件包解密，并核对文件包中的散列信息域。如果核对失败，接收方通知服务器这个决定，此时，加密文件或它的散列信息、共用封印、时间标志和终止目期都没有解密；

11.然后文件包重新加密并储存在接收方的使用目录密钥的专有目录中。

查看文件的操作程序如下：

1.接收方使用他们的用户名和口令注册到客户软件，并由硬件设备鉴别；

2.鉴别成功后，客户软件读取接收方的目录密钥，并访问接收方的有文件包的专有目录；

3.结束时间与硬件设备的内部时钟比较，如果内部时钟显示出结束时间已过去，则文件已经结束，不再允许访问；

4.如果文件没有结束，则接收方能访问文件。

打印文件的步骤如下：

1.接收方使用他们的用户名和口令注册客户软件，并由硬件设备鉴别；

2.鉴别成功后，客户软件读取接收方的目录密钥，并访问接收方的有文件包的专有目录；

3.客户软件将未使用的许可证发送给用该硬件设备用于解密；

4.硬件设备根据索引从接收方的DAR存储器读取密钥，并将会话密钥1和独特封印解密；

5. 将文件或其散列信息、共用封印、时间标志、终止目期发送给该设备用于解密。将终止目期与该设备中的时钟比较，如果内部时钟显示出终止目期已过，则文件已经逾期，不再允许打印；如果设备上的硬件有故障，用户应该要求硬件发放者来解决问题；

6.客户软件利用上述步骤（5）的解密文件散列信息验证文件的完整性，并将文件发送到打印机，或将解密文件发送到打印机；

7.客户软件与打印机通信，监视打印状态，将具有正确的封印的文件打印出来；

8.在每打印一份副本后，就进行核查跟踪信息，并利用接收方ID密钥由硬件设备内的程序签名，其保证认可打印副本；

9.硬件设备定期核对ID列表，以除去过期的ID;

10.将核查跟踪信息储存在硬件中，并定期装载到服务器。在预定时期内，服务器保持核查跟踪。在预定时期结束后，就从服务器删除。

如果硬件设备的CPU设有足够能力执行所有的加密/解密操作，或接口速度不足以满足打印要求，则硬件设备在打印过程中用作保密储存装置，如图12所示。该硬件设备包括:

1.保密存储器（1201），用来储存重要信息。当输入用户口令并得以证实时便可访问该存储器。用户ID密钥和/或系列号被储存在该存储器中，系列号最好由硬件厂商保证是唯一的。当使用数字证明时，用户的专有密钥可被储存在硬件设备中;

2.接口（1202），负责在硬件设备和主机之间建立通信，也将数据流加密，以防止线路分接攻击;

3.一个可选硬件时钟，具有备用电池（1203），当需要一定时间高度机密操作时，提供一个时基。

由于在先前的方案中，硬件设备并不是强功效的，所以，许可密钥安装和管理过程可由客户方的软件实现，并可由接口的防线路分接攻击功能予以保护。

硬件设备可通过该机器的USB端口、串行端口或并行端口连接到客户机上。许多现成的保密设备如智能卡、USB密钥、或并行端口硬件锁(dongle)，可用做硬件设备。每个用户都有他们自己的硬件设备，当需要时可连接到用户机器，并在使用后从用户机上拆卸下来。

服务器处于可信地位，可在作为发送方中心模式的发送方。也可作为独立的可信方。服务器的管理者负责发送硬件设备给用户，以及负责管理用于硬件设备的密钥。

硬件设备控制打印过程，方案如下:

方案1:

该方案使用了对称加密技术，例如，3DES，AES，Blowrish等等。它包括发送方、接收方、打印设备和可信服务器，如图13所示。

在接收方的硬件设备中的保密存储器中具有一组自由密钥（密钥1，...密钥N，T密钥），这些密钥是许可证密钥，并被用于给独特的封印加密。这些T密钥（添加密钥）被用在添加过程中。所有这些密钥的副本也保存在可信服

务器中。发送方和接收方，还有它们的硬件设备也都必须在利用保密打印过程之前利用可信服务器注册。

接收方的注册过程比上述注册过程要容易，包括:

1.接收方通过提供他们的信息，如用户名、电子邮件，请求在服务器注册;

2.服务器系统为接收方定制硬件设备，其保密存储器中具有独特的ID密钥、一系列许可证密钥和添加密钥。然后将这些密钥的副本记录在服务器的数据库中。并将初始口令指定给设备;

3.将设备和初始口令分别发送给接收方，并且如果先前没有安装客户软件的话，还将客户软件安装在接收方的机器上;

4.接收方通过输入他们的用户名和初始口令注册到客户软件;

5.将初始口令发送到该硬件设备用于验证，如果口令正确，则提示接收方改变他们的口令;

6.用新口令取代原始口令;

7.客户软件为用户准备一个专有目录，并将该目录的密钥（称做目录密钥）存储到硬件设备的保密存储器里。

许可证密钥添加过程

当设备随机密钥全部使用，或当对于新任务的许可证不足时，将有需要添加他们的随机密钥，步骤如下:

1.当服务器接收到发送方的请求，为一个文件发送M个许可证密钥给接收方，服务器会核对接收方的许可证密钥的使用情况，如需要时，服务器会启动添加过程；或者

2.接收方请求添加他们的许可证密钥，如接收方不具有足够的密钥，所有的接收方密钥都已使用，或接收方需要打印更多的副本;

3.然后，服务器处理该请求。如果批准的话，服务器就产生一组新的密钥密钥1′- 密钥X′，和一个新的添加密钥（T密钥′）;

4. 该组新的密钥用接收方的T密钥′加密;

5.为该组新的密钥计算散列信息，并利用接收方的ID密钥将其与加密的新密钥集加密，以形成添加密钥集;

6.添加密钥集与文件包一起或单独地发送给接收方;

7.在接收方检索文件包后，接收方将添加密钥集发送给硬件设备;

8.该设备用ID密钥给文件包解密，并为核对完整性而计算数据的散列信息；

9.如果有错误，该设备则从保密存储器读取T密钥以解密该密钥集；

10.然后硬件设备更新保密存储器中的密钥集。新的密钥集将不改写未使用的密钥，由于它的索引号从先前最后的密钥是连续的；

11.在保密存储器中的添加密钥（T密钥）由新添加密钥T密钥′来取代。

发送方将文件发送给接收方：

1.发送方利用他们的用户ID和口令通过保密链路（如SSL）连接到可信服务器；

2.鉴别成功后，发送方准备他们的文件：

a)使用会话密钥1将文件或它的散列信息结果、共用封印、用来发送的时间标志以及文件的终止日期加密；

b)为文件主体、终止日期和步骤a)的结果计算散列信息结果，然后将这三部分用会话密钥2加密；

c)然后将步骤b)的结果、接收方的ID、会话密钥1、用于加密的会话密钥2、关于接收方打印M份文件的许可证数量（如M）以及M个独特封印发送给服务器。M可能是0，表示只能查看；

3.服务器核对接收方信息，然后随机地或从接收方密钥集中顺序地选择M个许可证密钥（密钥1-密钥M）；

4.M个独特封印和会话密钥1各用密钥1-密钥M加密，形成M个许可证。计算每个许可证的散列信息域以对每个许可证核对完整性；

5.然后服务器产生一个文件包（图14），该包包括发送方准备好的文件包（上面步骤2中（b）的结果），用接收方ID密钥加密的会话密钥2以及许可证。如果发送方不允许接收方打印文件，关于许可证的域和添加密钥集将是空的。如果接收方的许可证密钥不够时，预备添加密钥集；

6.服务器通知接收方，告诉他们准备收集文件包。

接收方不管是否接到通知，都能连接到服务器，来核对是不是有给他们的数据。接收方查看并打印文件的操作程序如下：

1.接收方利用他们的用户名和口令，通过保密链路（如SSL）连接到可信服务器；

2.服务器通过发送询问响应系列验证用户：

a)服务器验证用户名，然后从数据库检索用户ID密钥；

b)服务器选择或产生随机号，利用用户ID密钥加密所述随机号，并将其发送给接收方。

c) 将接收方的口令发送给硬件设备，以访问用户的ID密钥；

d)硬件设备使用ID密钥将已加密的随机号解密；

e)将随机号向回发送给服务器；

f)服务器通过验证随机号来鉴别用户；

3.鉴别成功后，客户软件从服务器为接收方下载数据；

4.接收到数据后，接收方可与服务器断开，或保持在线状态；

5.客户软件核对是否有添加密钥集。如果有，则为了添加许可证密钥，首先将添加密钥集发送到设备；

6.客户软件将加密后的会话密钥2发送到用该硬件设备用于解密。解密的会话密钥2并从该硬件设备返回，该客户软件给文件包解密，并核对文件包中的散列信息域。如果核对失败，接收方通知服务器解决这个问题，此时，被加密的文件或它的散列信息、共用封印、时间标志和终止目期都没有解密；

然后使用目录密钥将文件包储存在接收方的专有目录中。

为接收方查看文件，执行以下操作程序：

1.接收方使用他们的用户名和口令注册到客户软件，并由硬件设备鉴别；

2.鉴别成功后，客户软件读取接收方的目录密钥，并访问接收方的有文件包的专有目录；

3.终止目期与硬件设备的内部时钟比较，如果内部时钟显示出终止目期已过去，则文件已经结束，不再允许访问；

4.如果文件没有结束，则接收方能访问文件。

当接收方打印文件时，执行以下步骤：

1.接收方使用他们的用户名和口令注册客户软件，并由硬件设备鉴别；

2.鉴别成功后，客户软件从硬件设备中读取接收方的目录密钥，并访问接收方的关于文件包的专有目录；

3.客户软件选择打印许可证，如果不能获得许可证，则不允许打印；

4.硬件设备从保密存储器读取许可证密钥，给会话密钥1和独特封印解密，并删除已使用过的许可证密钥；

5.用会话密钥1将文件或其散列信息、共用封印、时间标志、终止目期解密。将终止目期与该设备中的时钟比较，如果内部时钟显示出终止目期已过，则文件已经逾期，不再允许打印；如果设备上的硬件有故障，用户应该通知硬件发放者来解决问题；

6.客户软件利用上述步骤（5）的解密文件散列信息验证文件的完整性，并将文件发送到打印机，或将解密文件发送到打印机；

7.客户软件与打印机通信，监视打印状态，将具有正确的封印的文件打印出来；

8.在每打印一份副本后，就进行核查跟踪信息，并利用具有接收方ID密钥签名，以保证认可打印的副本；

9. 核查跟踪信息储存在硬件中，并定期装载到服务器。在预定时期内，服务器保持核查跟踪。在预定时期结束时，就将核查跟踪信息删除。

方案2:

如图17所示，当硬件设备中的保密存储器制造出来时是空的（记为零）。所有发送方和接收方以及他们的硬件设备，必须在利用本发明的保密打印过程之前，一起利用可信服务器注册。

接收方的注册过程比上述注册过程要容易，包括:

1.接收方通过提供他们的信息，如用户名、电子邮件地址，请求在服务器注册；

2.服务器系统为接收方定制硬件设备，其存储器中具有独特的ID密钥。然后将ID密钥的副本记录在服务器的数据库中，并为硬件设备指定初始口令；

3.将硬件设备和初始口令分别发送给接收方，并且将客户软件安装在接收方的机器上；

4.接收方通过输入他们的用户名和初始口令注册到客户软件；

5.将初始口令发送到硬件设备用于验证，如果口令正确，则提示接收方改变他们的口令；

6.用新口令取代原始口令；

7.客户软件为用户准备一个专有目录，并将该目录的密钥（称做目录密钥）存储到硬件设备的保密存储器中。

用户发送文件的操作程序如下:

1.发送方使用他们的用户ID和口令通过保密链路（如SSL）连接到可信服务器；

2.鉴别成功后，发送方准备他们的文件：

a)使用会话密钥1将文件或它的散列信息结果、共用封印、用于发送的时间标志以及文件的终止目期加密；

b)为文件主体、终止目期和步骤a)的结果计算散列信息结果，然后将这三部分用会话密钥2加密；

c)然后将步骤b)的结果、接收方的ID、会话密钥1、用于加密的会话密钥2、关于接收方打印M份文件副本的许可证数量（如M）以及M个独特封印发送给服务器。M可能是0，表示只能查看；

3.服务器核对接收方信息，然后产生一个许可证和许可证安装程序，如图19所示；

4.许可证包含会话密钥1和M个独特封印，该M个独特封印用M个服务器随机地产生的许可证密钥密钥1-密钥M加密；

5.许可证安装程序包含一个用于文件的独特ID，也包含一个时间标志（此时，产生许可证安装程序）和终止目期，该许可证安装程序利用接收方ID密钥加密；

6. 计算许可证和许可证安装程序的散列信息，以核对其完整性；

7.然后服务器产生一个文件包，如图18所示，该包包括发送方准备好的文件包（上面步骤2中（b）的结果），用接收方ID密钥加密的会话密钥2以及许可证、许可证安装程序。如果发送方不允许接收方打印文件，许可证和许可证安装程序的域将是空的；

8.服务器通知接收方，告诉他们准备收集文件包。

不管接收到还是没有接收到任何这样的通知，接收方都能连接到服务器，核对是不是有给他们的文件。接收方查看并打印文件的操作程序如下：

1.接收方利用他们的用户名和口令，通过保密链路（如SSL）连接到可信服务器；

2.服务器通过发送询问响应系列验证用户：

a)服务器验证用户名，然后从数据库检索用户ID密钥；

b)服务器选择或产生随机号，利用用户ID密钥加密所述随机号，并将其发送给接收方。

c) 将接收方的口令发送给硬件设备，以访问他们的ID密钥；

d)硬件设备使用ID密钥将已加密的随机号解密；

e)将随机号向回发送到服务器；

f)服务器通过验证随机号来鉴别用户；

3.鉴别成功后，接收方为他们从服务器下载数据；

4.接收到数据后，接收方可与服务器断开，或保持在线状态；

5.客户软件将许可证安装程序发送给接收方硬件设备，以实现安装；

6.硬件设备使用接收方ID密钥将许可证安装程序解密，并通过验证散列信息域而核对许可证安装程序的完整性。如果验证失败，则接收方通知服务器解决问题；

7.该硬件设备利用硬件设备中保存的ID列表，核对文件ID；如果没发现ID，就依靠在设备中的时钟核对时间标志和终止目期；

8.如果所有核对过程完成得都很成功，则许可证密钥就被安装在保密存储器中，并且ID被储存在保密存储器的ID列表中；

9.客户软件将加密会话密钥2发送到用该硬件设备用于解密。该硬件设备将会话密钥2解密，并返回客户软件，该客户软件给文件包解密，并核对文件包中的散列信息域。如果核对失败，接收方通知服务器解决问题，此时，被加密的文件或它的散列信息、共用封印、时间标志和终止目期都没有解密；

10.然后使用目录密钥，将文件包重新加密并储存在接收方的专有目录中。

接收方查看文件的操作程序如下：

1.接收方使用他们的用户名和口令注册到客户软件，并由硬件设备鉴别；

2.鉴别成功后，客户软件读取接收方的目录密钥，并访问接收方的文件包的专有目录；

3.将终止目期与硬件设备的内部时钟比较，如果内部时钟显示出终止目期已过，则文件已经逾期，不再允许访问；

4.如果文件没有逾期，则接收方能查看文件。

接收方打印文件的步骤如下：

1.接收方使用他们的用户名和口令注册到客户软件，并由硬件设备鉴别；

2.鉴别成功后，客户软件读取接收方的目录密钥，并访问接收方的文件包的专有目录；

3.客户软件选择未使用的许可证，如果不能获得打印许可证，就不允许打印；

4. 如果能获得未使用过的打印许可证，客户软件就将许可证发送给用该硬件设备用于解密。该设备从保密存储器读取许可证密钥，并将会话密钥1和独特封印解密；

5. 将文件或其散列信息、共用封印、时间标志、终止目期发送给用该硬件设备用于解密。将终止目期与该设备中的时钟比较，如果内部时钟显示出终止目期已过，则文件已经逾期，不再允许打印；如果设备上的硬件有故障，用户应该通知硬件发放者来解决问题；

6.设备删除已使用过的许可证密钥；

7.客户软件利用上述步骤(5)的已解密文件散列信息验证文件的完整性，并将文件发送到打印机，或将解密文件发送到打印机；

8.客户软件与打印机通信，监视打印状态，将具有正确的封印的文件打印出来；

9.在每打印一份副本后，进行核查跟踪信息，并利用接收方ID密钥签名，以保证认可打印的副本；

10 客户软件定期核对设备内的ID列表，以除去过期的ID；

11. 将核查跟踪信息储存在硬件设备中，并定期下载到服务器。在预定时期内，服务器保持核查跟踪信息。在预定时期结束后，就将核查跟踪信息删除。

脱机打印控制-软件方案

在这种情形下，不需要附加的硬件来控制打印。相反，每个接收方安装有软件代理程序(agent)，如图20所示。

软件代理程序最好用各种技术例如防修改、防调试(debug)技术等等来得以保护，一系列密钥都被储存在密钥数据库（如图20）中，该系列密钥用于具有独特文件ID和独特ID密钥的不同打印许可证，该数据库是一个位于客户当地硬盘上的文件。这些密钥由具有写密码功能的软件代理程序内部使用。软件代理程序还为每个用户保留一个专有目录，该目录受到用户ID密钥的保护。当使用数字证明时，用户ID密钥可以是用户的专有密钥。

密钥数据库文件用保密密钥加密。软件代理程序将保密密钥储存在保密储存器中。例如，可将密钥分配在硬盘的各个位置，这就使密钥数值的再生容易成功，对软件代理程序的相反操纵十分困难。

在几个条件下，不兼容的磁盘可能偶然毁坏保密存储器。引入挽救机理来解决这个问题。在用户利用服务器注册时，服务器将产生一个挽救密钥对。密钥对的公用密钥部分将安装在接收方的机器上，同时，专有挽救密钥将保持在服务器数据库中。软件代理程序将保留保密密钥的副本，该保密密钥用挽救公用密钥加密，如挽救文件（图21）。如果保密密钥丢失，软件代理将与服务器通信，通过使用挽救文件来使保密密钥再生。

基于软件的脱机打印控制的工作情况与基于硬件的控制方案2一样，如上所述。

发送操作程序如下：

1.发送方使用他们的用户ID和口令通过保密链路（如SSL）连接到可信服务器；

2.鉴别成功后，发送方准备他们的文件：

a)使用会话密钥1将文件或其散列信息、共用封印、用于发送的时间标志以及文件的终止日期加密；

b)为文件主体、终止日期和步骤a)的结果计算散列信息结果，然后将这三部分用会话密钥2加密；

c)然后将步骤b)的结果、接收方的ID、会话密钥1、用于加密的会话密钥2、关于接收方打印M份副本的许可证数量（如M）以及M个独特封印发送给服务器。M可能是0，表示只能查看；

3.服务器核对接收方信息，然后产生一个许可证和许可证安装程序，如图23所示；

4.许可证包含会话密钥1和M个独特封印，该M个独特封印用服务器随机地产生的M个许可证密钥密钥1-密钥M加密；

5.许可证安装程序包含一个用于文件的独特ID，也包含一个时间标志（此时，产生许可证安装程序）和终止日期，该许可证安装程序是利用接收方ID密钥加密的；

6. 计算许可证和许可证安装程序的散列信息，以核对其完整性；

7.然后服务器产生一个文件包，如图24所示，该包包括发送方准备好的文件包（上面步骤2中（b）的结果），用接收方ID密钥加密的会话密钥2以及许可证、许可证安装程序。如果发送方不允许接收方打印文件，许可证和许可证安装程序的域将是空的；

8 服务器通知接收方准备收集文件包。

不管接收到还是没有接收到任何这样的通知，接收方都可连接到服务器，核对是不是有给他们的文件和/或数据。接收方查看并打印文件的操作程序如下：

1.接收方利用他们的用户名和口令，通过保密链路（如SSL）连接到可信服务器，并由软件代理程序鉴别；

2.鉴别成功后，接收方从服务器为自己下载数据；

3.接收到数据后，接收方可与服务器断开，或保持在线状态；

4.客户软件将许可证安装程序发送给软件代理程序；

5.软件代理使用ID密钥将许可证安装程序解密，并核对其完整性。如果完整性验证失败，则接收方通知服务器解决问题；

6.该设备利用保存在密钥数据库中的ID列表，核对文件ID；

7.如果不匹配，依靠设备中的时钟核对时间标志和终止目期。如果终止目期已过，则不会安装许可证；

8.如果成功完成所有核对过程，则将许可证密钥安装在密钥数据库中，并且将ID储存在ID列表中；

9.客户软件将加密后的会话密钥2发送到软件代理程序用于解密。该软件代理程序将会话密钥2解密，并返回客户软件，该客户软件将文件包解密，并核对其完整性。如果核对失败，接收方通知服务器解决这个问题；否则将文件包储存在接收方专有目录中。

接收方查看文件的操作程序如下：

1.接收方使用他们的用户名和口令注册到客户软件，并由软件代理鉴别；

2.鉴别成功后，软件代理访问接收方的文件包的专有目录；

3.将终止目期与系统时钟比较，如果系统时钟显示出终止目期已过，则文件已经逾期，不再允许查看；

4.如果文件没有逾期，则接收方能查看文件。

接收方打印文件的步骤如下：

1.接收方使用他们的用户名和口令注册到客户软件，并由软件代理程序鉴别；

2.鉴别成功后，软件代理程序访问接收方的文件包的专有目录；

3.客户软件选择未使用的打印许可证，并发送给软件代理程序。如果仍没有打印许可，则不允许打印；

4.如果有未使用的打印许可，软件代理程序就会根据许可证将会话密钥1和独特封印解密；

5. 使用会话密钥1将文件或其散列信息、共用封印、时间标志、终止目期解密。将终止目期与系统时钟比较，如果系统时钟显示出终止目期已过，则文件已经逾期，不再允许打印；

6.客户软件利用上述步骤（5）的解密文件散列信息验证文件的完整性，并将文件发送到打印机，或将解密文件发送到打印机；

7.客户软件与打印机通信，监视打印状态，将具有正确的封印的文件打印；

8.在每打印一份副本后，进行核查跟踪信息，并利用接收方ID密钥签名，以保证认可打印的副本；

9.客户软件定期核对密钥数据库中的ID列表，以除去过期的ID；

10. 核查跟踪信息被储存在密钥数据库中，并定期下载到服务器。在预定时期内，服务器保持核查跟踪信息。在预定时期结束后，就将核查跟踪信息删除。

11.客户软件产生一个新的保密密钥，并将密钥数据库再加密；

12.客户软件通过用挽救公用密钥将新保密密钥加密，而产生一个新密钥挽救文件；

在上述讨论中，为方便之见，可使用均衡密钥或公用密钥。在任一情况下，可使用均衡密钥和公用密钥两者。预定时期可由用户、服务器或两者之间的协议来设置。

除此之外，发送方和服务器可能是一个。如，发放管理机构可能是发送方和服务器，在这种情况下，服务器执行的是两者的功能。

正如所看见的一样，本发明涉及到鉴别文本的远程打印，该鉴别文本通过网络发送。这样可减少成本，放慢递送经鉴别的纸件文件的物理传送。在

一定领域中本发明运用时会产生相当大的优点。一个是保密打印行业中，他们都是可信和授权的代理。经鉴别的文件，如现金纸币和银行支票，都能使用特殊的打印机、特殊墨水、特殊用纸和其它特殊材料打印。打印过程和打印材料都是严格控制的。另一个是签署的文件，管理机构用他们的签名和/或封印启用文件。在两种情况下，签名和特殊的打印材料，增加文件可靠性，是完全受到经授权的个人或代理人控制的。

例如，如果发送方和接收方都是同一个，服务器可能是发放管理机构如邮政局的一部分，受控打印的是邮票。另一个例子是，当管理机构是售票代理处时，受控打印的是票，如用于音乐会、运动会、电影或此类的票。在有些国家，国内税收服务或其相关行业要将收据号发送给商业对象，并且正式收据必须为每一个收到的支付单而发放。这使得他们能保留商家收到的支付支票。这个打印控制的是收据号。

本发明也用于需要可信打印或发送文件的场合。这可包括税务发票或收据，这种情况下包含的步骤如下：

a)相关政府部门发放保密硬件设备给每个商家；

b)政府部门发放标准税收发票和/或收据格式，将许可证密钥发送给商家；

c)商家利用硬件设备来产生税收发票和/或收据，然后以电子形式或硬拷贝的形式发送给消费者。如果以电子形式发送，硬件设备控制发送过程与以硬拷贝打印相同的方式进行；

d)硬件设备进行核查跟踪信息，并记录下所有必要数据，该数据包括每个收据和发票的数量；

e)当许可密钥添加时，核查跟踪信息被发送到政府部门。在这个基础上，政府部门依据从核查跟踪系统获得的信息来决定每个商家应支付的税款。

虽然上述说明中描述了本发明的最佳实施例，可以理解的是，对于本领域技术人员来讲，在不脱离本发明实质的情况下可以对细节作出改变或修正。

本发明可扩展到每个公开的各个特征，这些特征中的所有可能的置换以及综合。

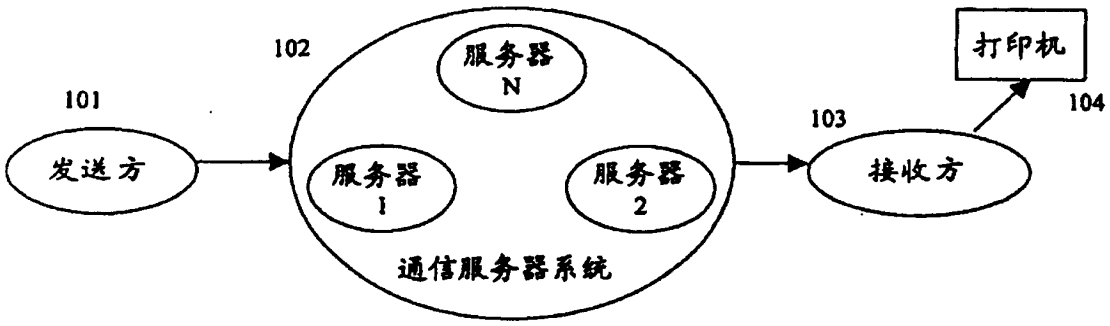


图 1

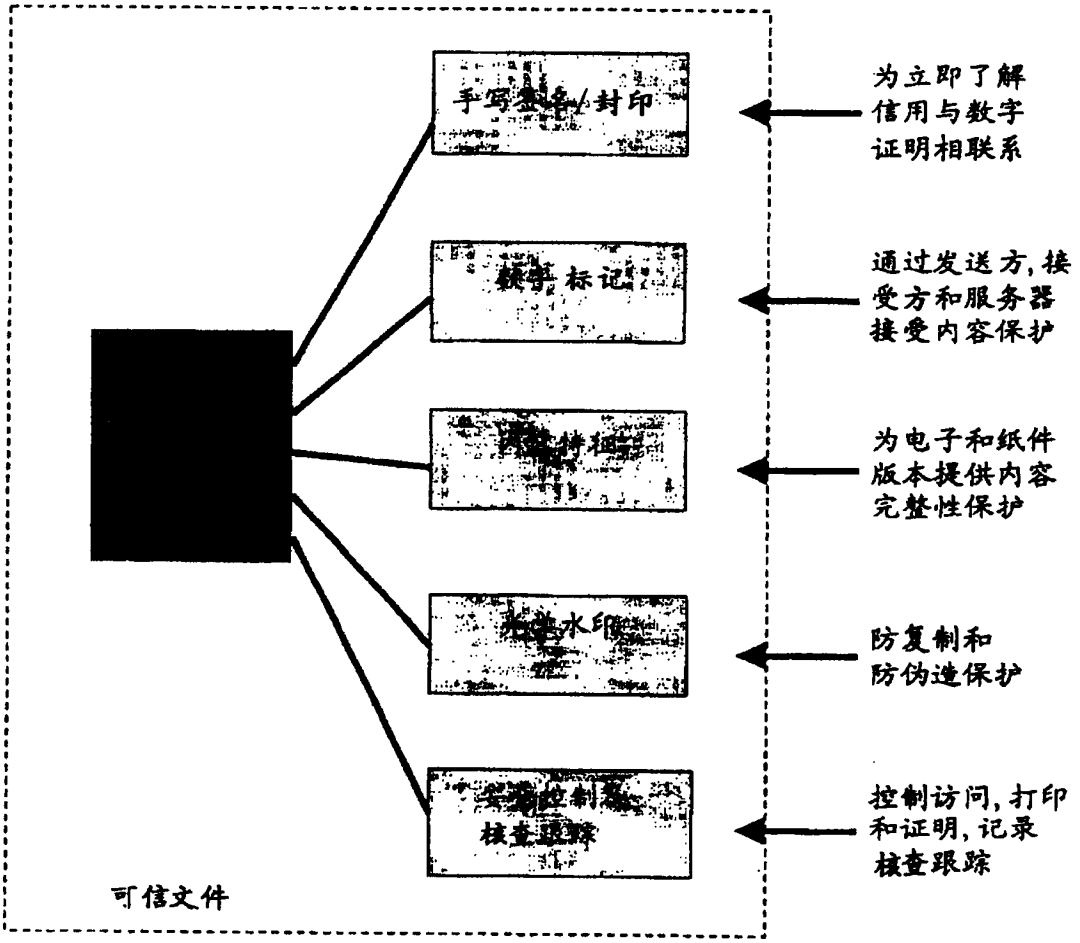

手写签名/封印
为立即了解
信用与数字
证明相联系
通过发送方，接
受方和服务器
接受内容保护
为电子和纸件
版本提供内容
完整性保护
防复制和
防伪造保护
控制访问，打印
和证明，记录
核查跟踪
可信文件

图 2

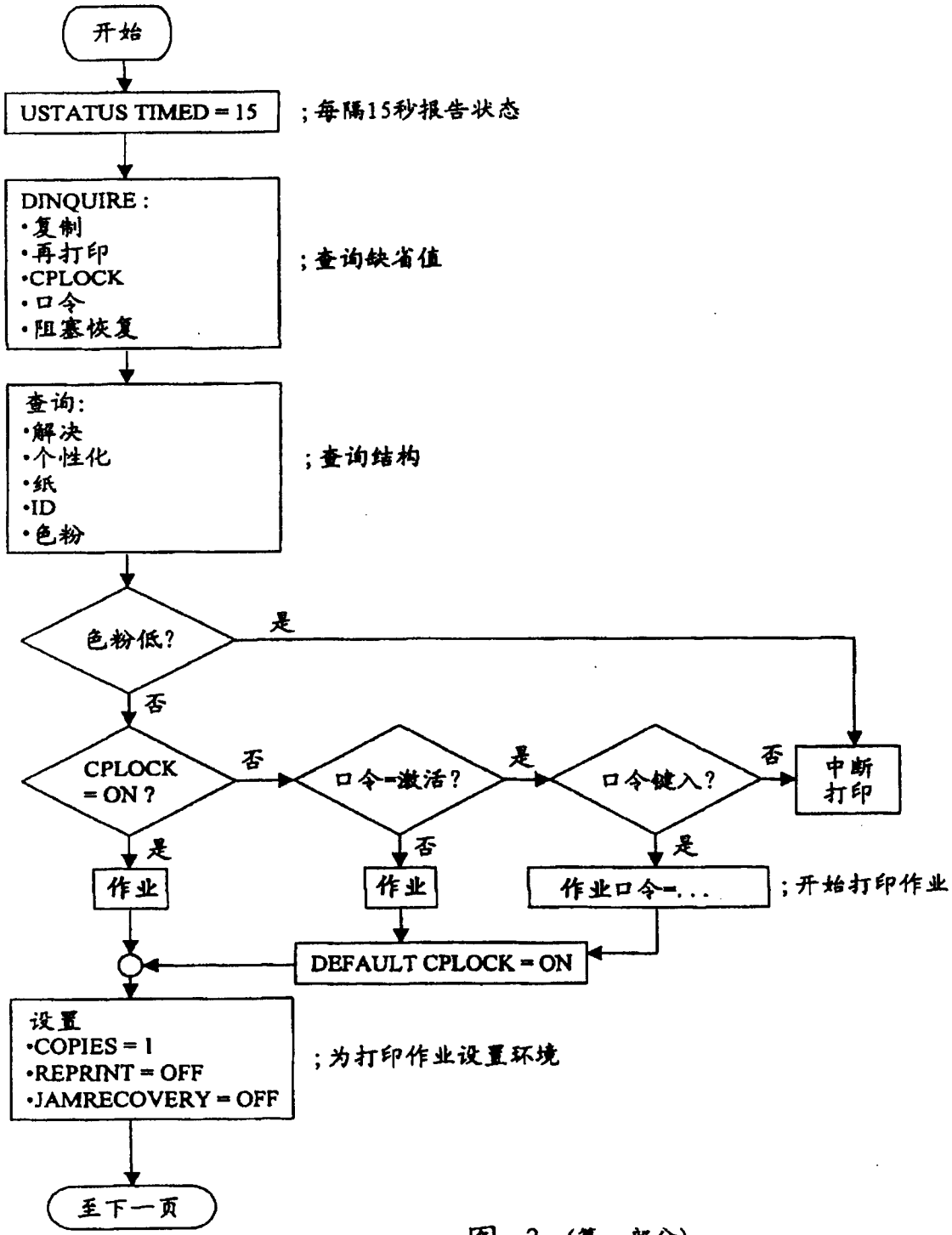

开始
USTATUS TIMED = 15
；每隔15秒报告状态
DINQUIRE：
•复制
•再打印
•CPLOCK
•口令
•阻塞恢复
；查询缺省值
查询：
•解决
•个性化
•纸
•ID
•色粉
；查询结构
色粉低？
是
否
CPLOCK = ON？
否
口令=激活？
是
口令键入？
否
中断打印
是
否
是
作业
作业
作业口令=...
；开始打印作业
DEFAULT CPLOCK = ON
设置
•COPIES = 1
•REPRINT = OFF
•JAMRECOVERY = OFF
；为打印作业设置环境
至下一页

图 3 （第一部分）

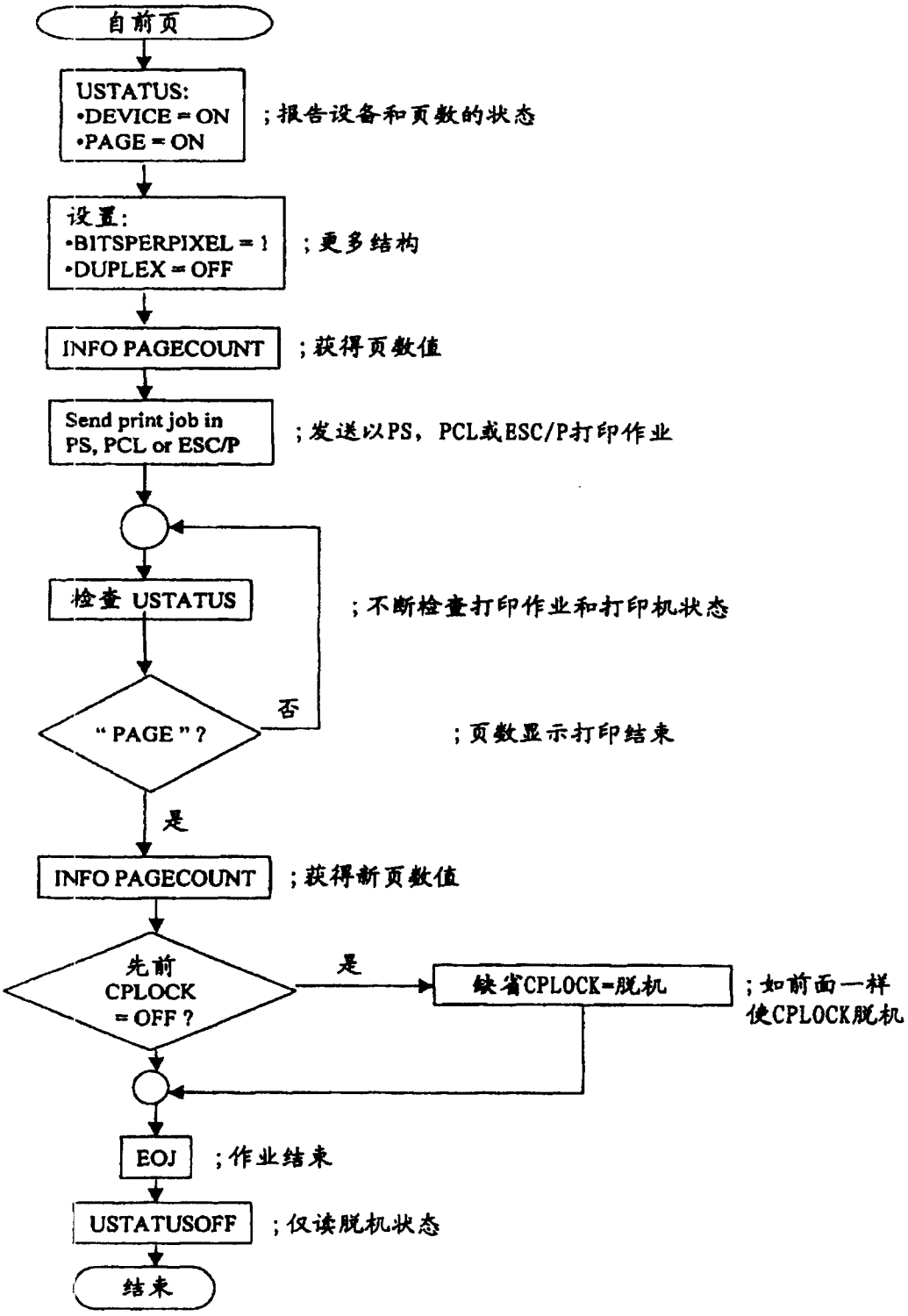

自前页
USTATUS:
•DEVICE = ON
•PAGE = ON
；报告设备和页数的状态
设置:
•BITSPERPIXEL = 1
•DUPLEX = OFF
；更多结构
INFO PAGECOUNT
；获得页数值
Send print job in
PS, PCL or ESC/P
；发送以PS，PCL或ESC/P打印作业
检查 USTATUS
；不断检查打印作业和打印机状态
“PAGE”?
否
；页数显示打印结束
是
INFO PAGECOUNT
；获得新页数值
先前
CPLOCK
= OFF ?
是
缺省CPLOCK=脱机
；如前面一样
使CPLOCK脱机
EOJ
；作业结束
USTATUSOFF
；仅读脱机状态
结束

图 3 (第二部分)

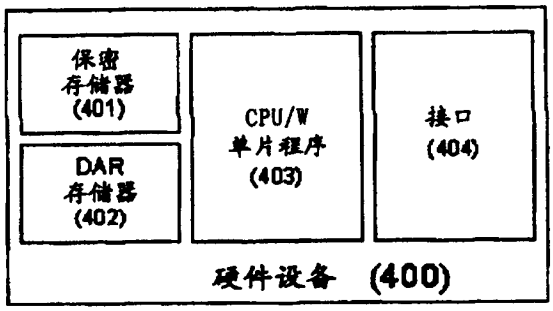

保密
存储器
(401)
DAR
存储器
(402)
CPU/W
单片程序
(403)
接口
(404)
硬件设备 (400)

图 4

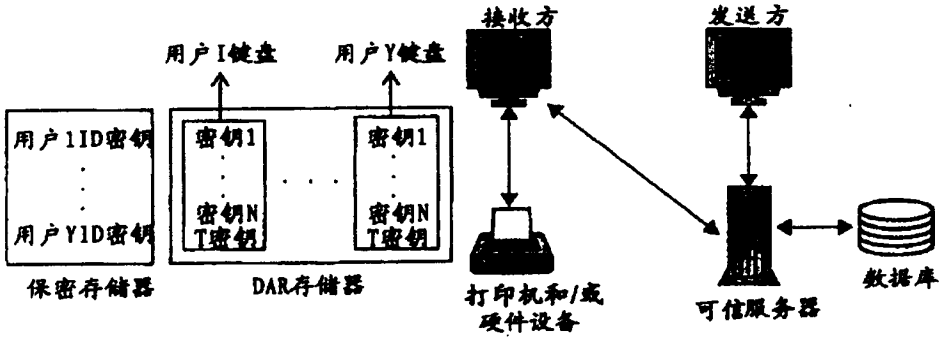

接收方
发送方
用户I键盘
用户Y键盘
用户1ID密钥
用户YID密钥
密钥1
密钥N
T密钥
密钥1
密钥N
T密钥
保密存储器
DAR存储器
打印机和/或
硬件设备
可信服务器
数据库

图 5

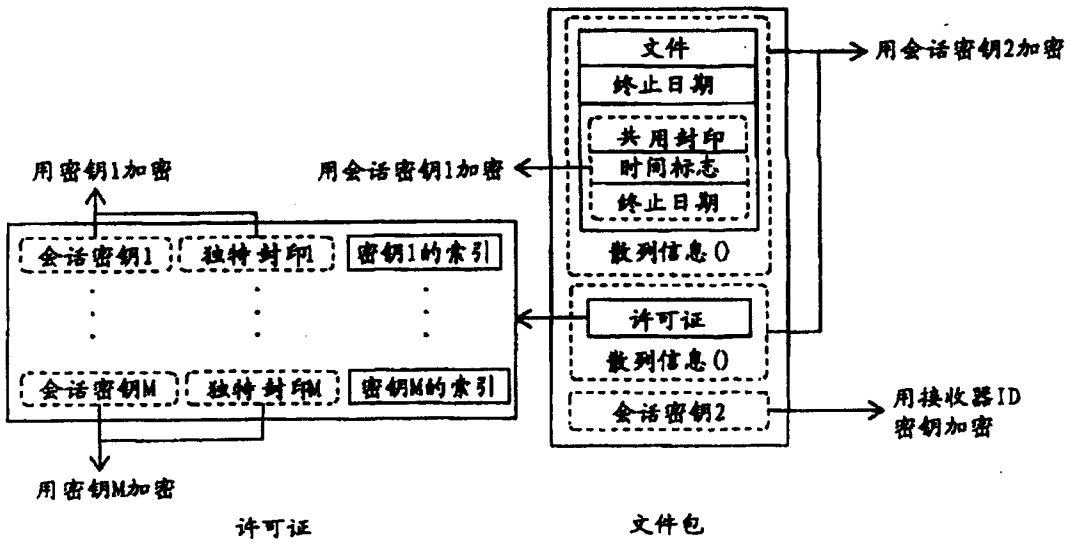

文件
终止日期
共用封印
时间标志
终止日期
散列信息O
许可证
散列信息O
会话密钥2
用会话密钥2加密
用接收器ID
密钥加密
用密钥1加密
用会话密钥1加密
会话密钥1
独特封印1
密钥1的索引
会话密钥M
独特封印M
密钥M的索引
用密钥M加密
许可证
文件包

图 6

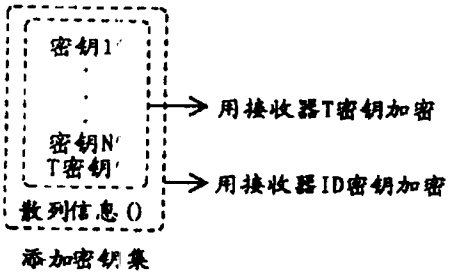

密钥1′
密钥N′
T密钥′
用接收器T密钥加密
用接收器ID密钥加密
散列信息 O
添加密钥集

图 7

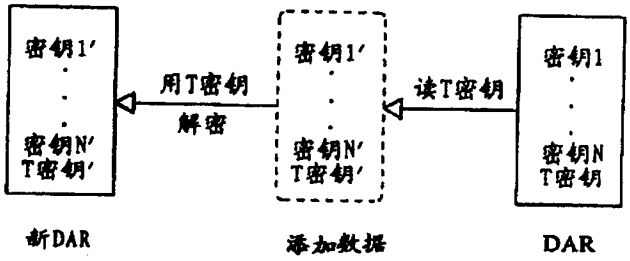

密钥1′
密钥N′
T密钥′
用T密钥
解密
密钥1′
密钥N′
T密钥′
读T密钥
密钥1
密钥N
T密钥
新DAR
添加数据
DAR

图 8

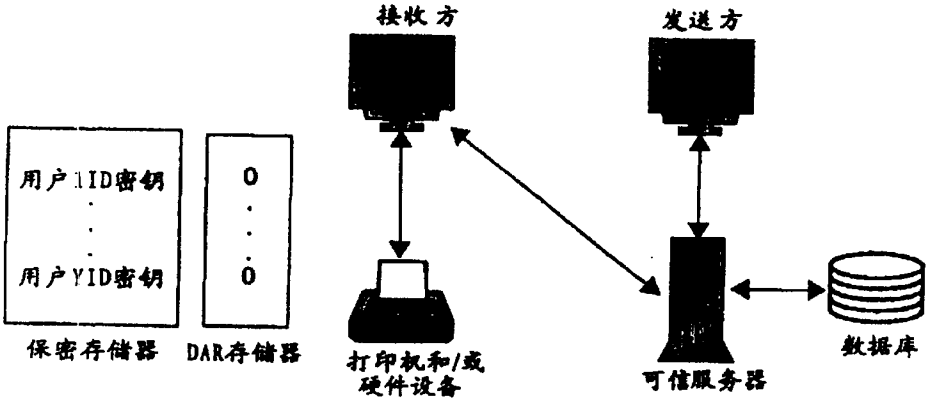

接收方
发送方
用户1ID密钥
用户YID密钥
保密存储器
0
0
DAR存储器
打印机和/或
硬件设备
可信服务器
数据库

图 9

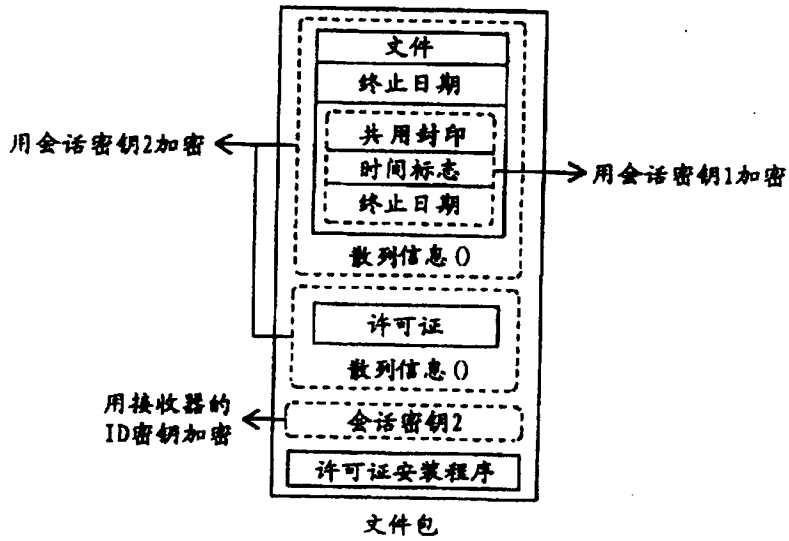

文件
终止日期
共用封印
时间标志
终止日期
散列信息 O
用会话密钥2加密
用会话密钥1加密
许可证
散列信息 O
用接收器的
ID密钥加密
会话密钥2
许可证安装程序
文件包

图 10

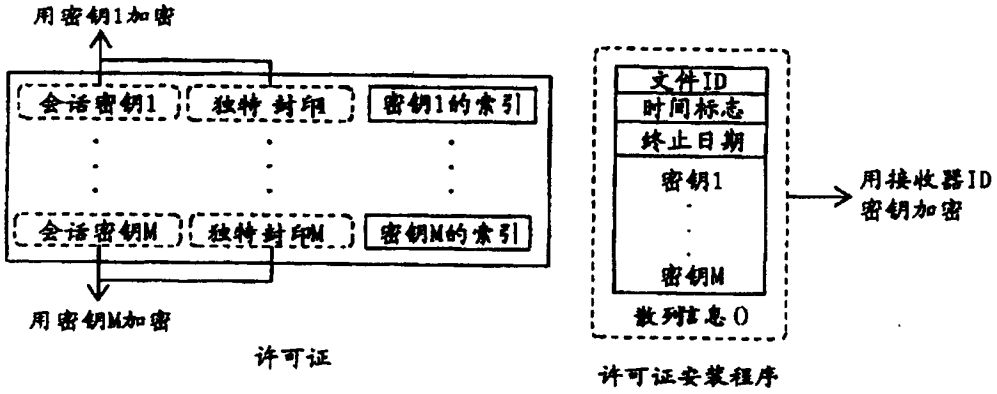

用密钥1加密
会话密钥1
独特封印
密钥1的索引
会话密钥M
独特封印M
密钥M的索引
用密钥M加密
许可证
文件ID
时间标志
终止日期
密钥1
密钥M
散列信息()
用接收器ID
密钥加密
许可证安装程序

图 11

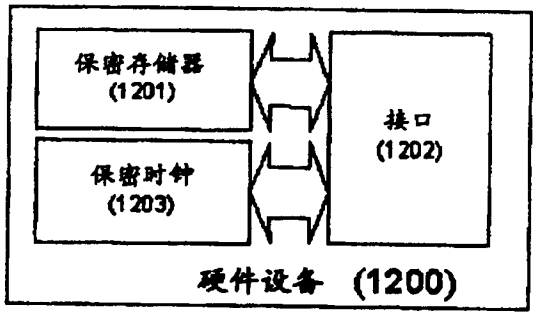

保密存储器
(1201)
保密时钟
(1203)
接口
(1202)
硬件设备 (1200)

图 12

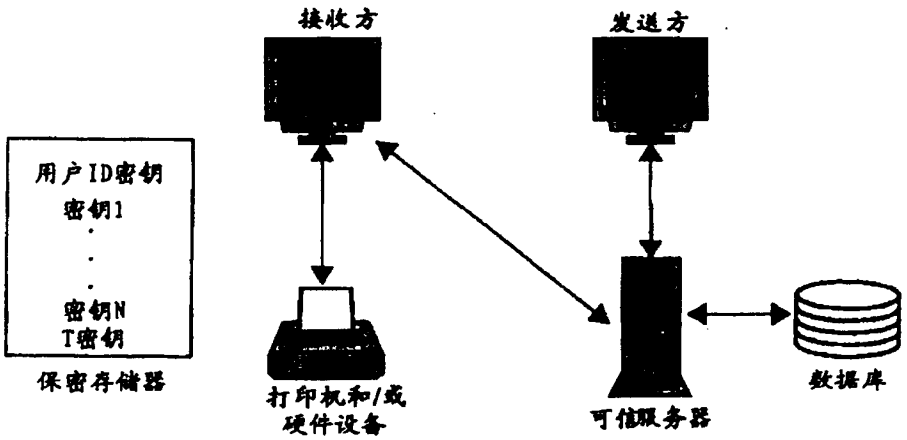

接收方
发送方
用户ID密钥
密钥1
密钥N
T密钥
保密存储器
打印机和/或
硬件设备
可信服务器
数据库

图 13

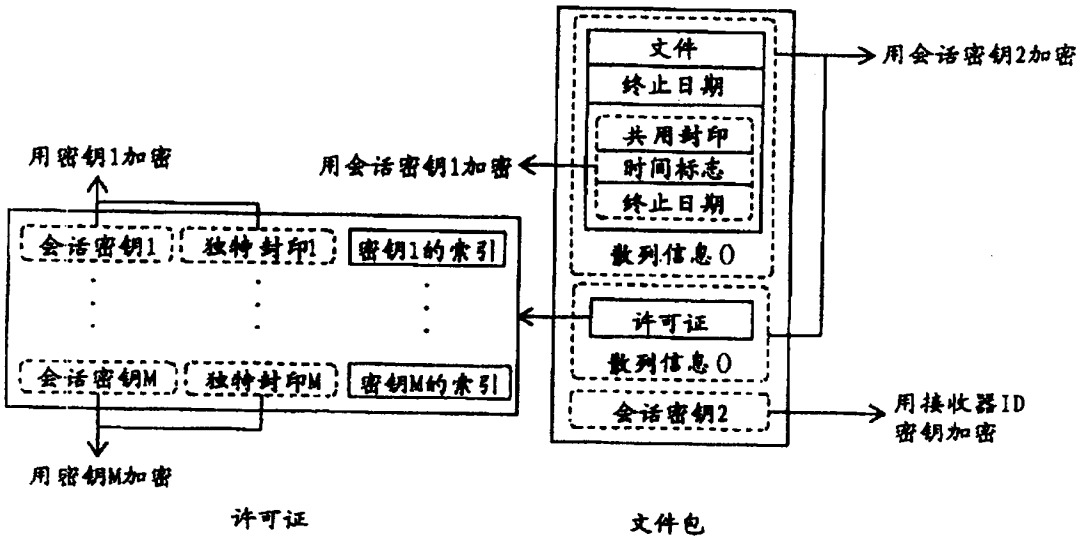


图 14

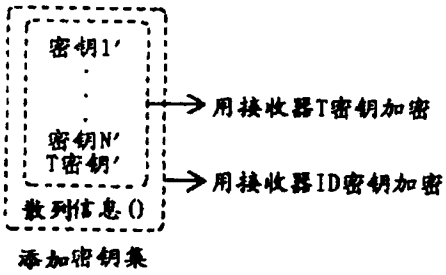


图 15

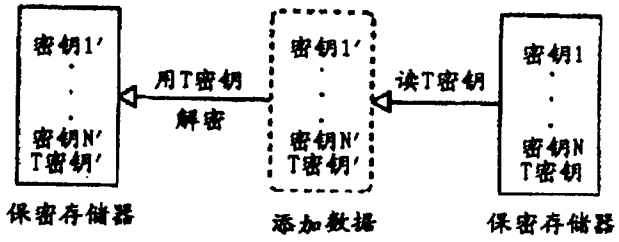


图 16

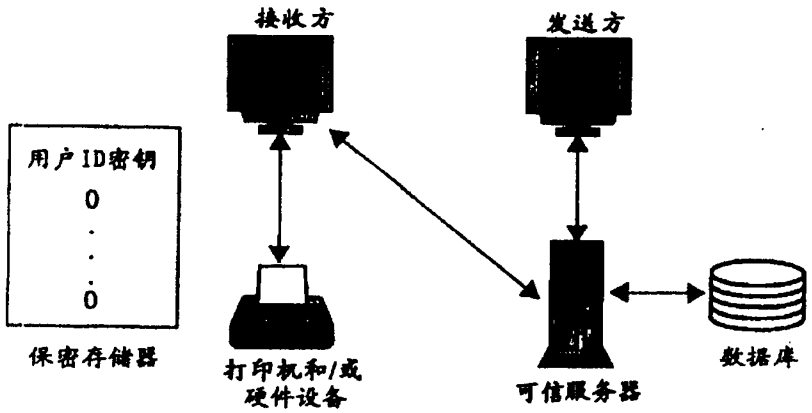


图 17

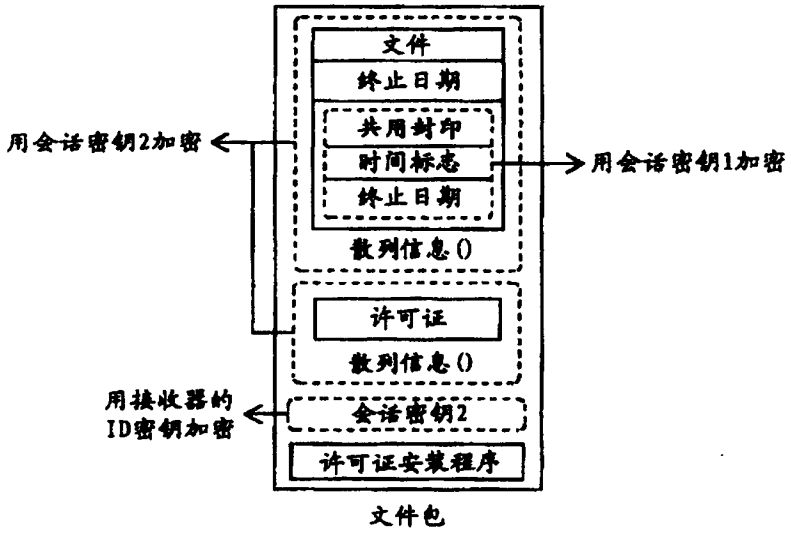

文件
终止日期
共用封印
时间标志
终止日期
散列信息()
许可证
散列信息()
会话密钥2
许可证安装程序
文件包
用会话密钥2加密
用会话密钥1加密
用接收器的
ID密钥加密

图 18

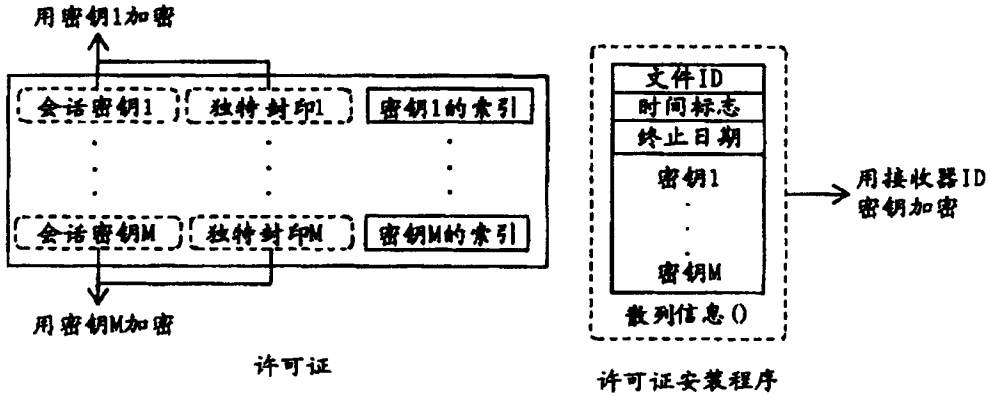

用密钥1加密
会话密钥1
独特封印1
密钥1的索引
会话密钥M
独特封印M
密钥M的索引
用密钥M加密
许可证
文件ID
时间标志
终止日期
密钥1
密钥M
散列信息()
许可证安装程序
用接收器ID
密钥加密

图 19

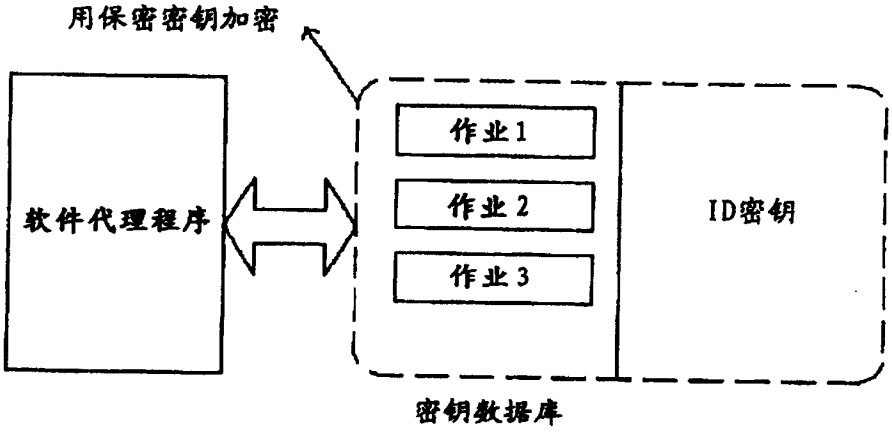


图 20

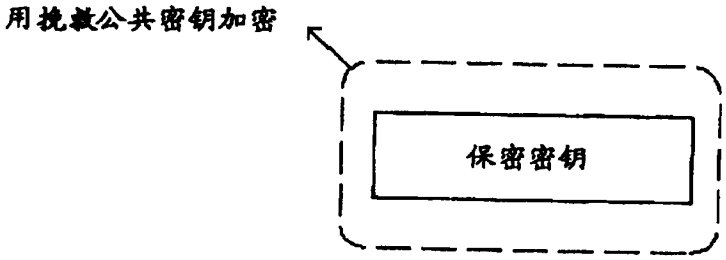


图 21

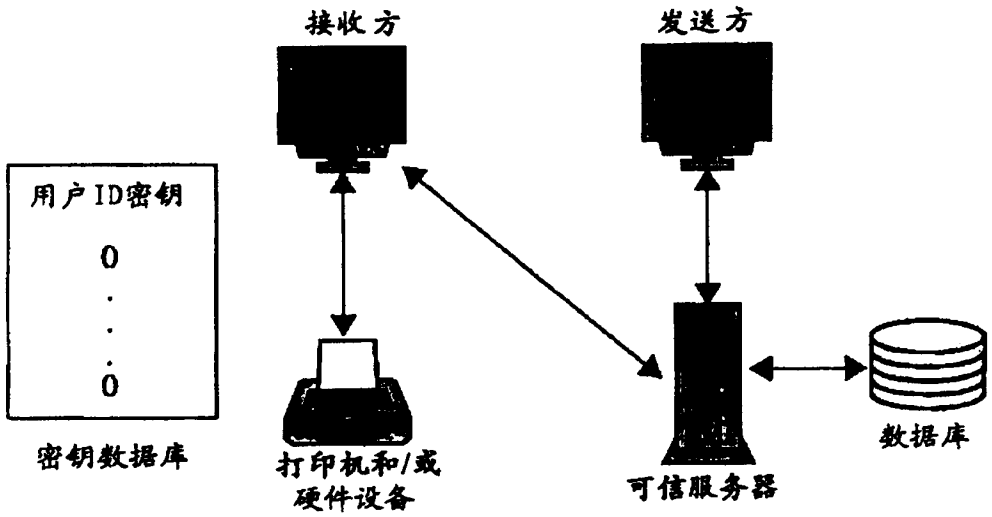

接收方
发送方
用户ID密钥
0
0
密钥数据库
打印机和/或
硬件设备
可信服务器
数据库

图 22

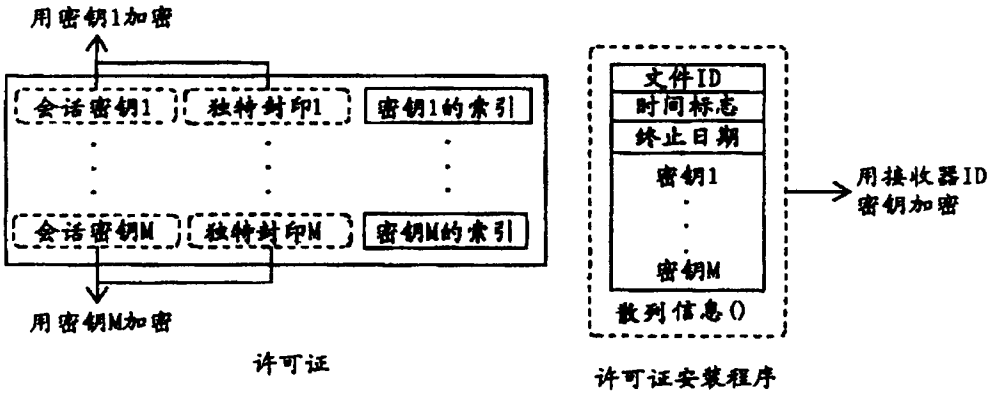

用密钥1加密
会话密钥1
独特封印1
密钥1的索引
会话密钥M
独特封印M
密钥M的索引
用密钥M加密
许可证
文件ID
时间标志
终止日期
密钥1
密钥M
散列信息()
用接收器ID
密钥加密
许可证安装程序

图 23

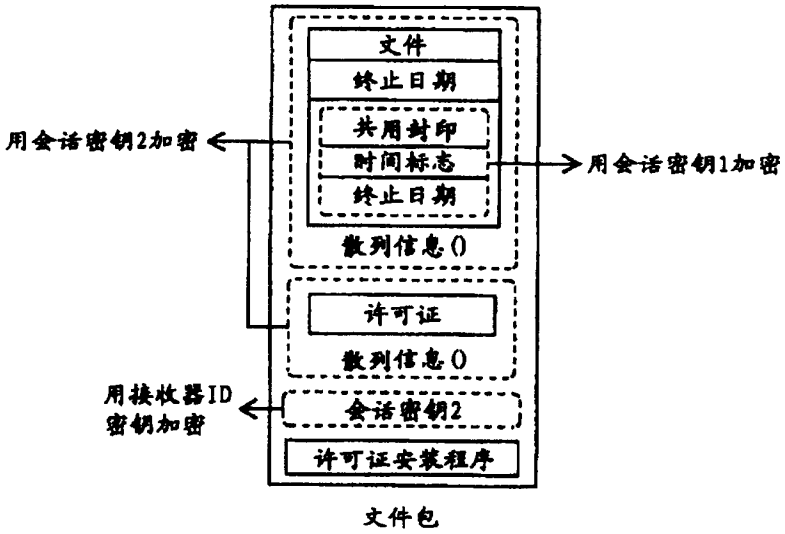

文件
终止日期
共用封印
时间标志
终止日期
散列信息0
许可证
散列信息0
会话密钥2
许可证安装程序
文件包
用会话密钥2加密
用会话密钥1加密
用接收器ID
密钥加密

图 24